

EDPS



EUROPEAN DATA PROTECTION SUPERVISOR

# EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data  
protection authority

## ANNUAL REPORT 2020



[edps.europa.eu](https://edps.europa.eu)

An executive summary of this report, which gives an overview of the key developments in EDPS activities in 2020, 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, 2021

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

© European Union, 2021

Reproduction is authorised provided the source is acknowledged.

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

PRINT ISBN 978-92-9242-618-7 ISSN 1830-5474 doi: 10.2804/67765 QT-AA-21-001-EN-C

PDF ISBN 978-92-9242-617-0 ISSN 1830-9585 doi: 10.2804/205036 QT-AA-21-001-EN-N

HTML ISBN 978-92-9242-616-3 ISSN 1830-9585 doi: 10.2804/548396 QT-AA-21-001-EN-Q



# ANNUAL REPORT 2020

# TABLE OF CONTENTS

<b>FOREWORD</b>	<b>12</b>
<b>MISSION, VALUES AND PRINCIPLES</b>	<b>14</b>
<b>EDPS STRATEGY 2020-2024</b>	<b>16</b>
<b>CHAPTER 1: ABOUT THE EDPS</b>	<b>18</b>
1.1 Supervision and Enforcement	19
1.2 Policy and Consultation	19
1.3 Technology and Privacy	20
1.4 The EDPS works on transversal issues	21
<b>CHAPTER 2: THE EDPS' 2020 HIGHLIGHTS</b>	<b>22</b>
2.1 Data protection in a global health crisis	22
2.2 EUIs' compliance with data protection law	23
2.3 Safeguarding digital rights	24
2.4 Monitoring technologies	25
2.5 The EDPS as a member of the EDPB	25
2.6 International cooperation in data protection	26
2.7 Internal administration	26
2.8 Communicating data protection	26
2.9 Key Performance Indicators	26
<b>CHAPTER 3: 2020 — AN OVERVIEW</b>	<b>30</b>
3.1 Data Protection amid a global health crisis	30
3.2 Safeguarding EU digital rights	33

3.3 Supervising European institutions, bodies and agencies (EUIs)	35
3.4 Supervising Area of Freedom, Security and Justice	45
3.5 Technology and Privacy	50
3.6 Legislative Consultations	59
3.7 The EDPS as a member of the EDPB	65
3.8 International Cooperation	67
3.9 Cooperation with Civil Society	69
<b>CHAPTER 4: TRANSPARENCY AND ACCESS DOCUMENTS</b>	<b>70</b>
<b>CHAPTER 5: THE SECRETARIAT</b>	<b>71</b>
5.1 Information and Communication	71
5.2 Administration, budget and staff	76
<b>CHAPTER 6. THE DATA PROTECTION OFFICER AT THE EDPS</b>	<b>83</b>
6.1 Accountability	83
6.2 Enquiries and complaints	84
6.3 Advising the EDPS	84
6.4 Awareness-raising	85
6.5 Collaboration with DPOs of other EUIs	85
<b>CHAPTER 7. ANNEXES</b>	
Annex A Legal Framework	86
Annex B Extract from Regulation (EU) 2018/1725	90
Annex C List of Data Protection Officers	94
Annex D List Of Opinions and Formal Comments	100
Annex E List of Consultations and Prior Consultations	104
Annex F Speeches by the Supervisor	106
Annex G The EDPS	112

## TABLES AND GRAPHS

Figure 1	EDPS KPI analysis table	28
Figure 2	Number of complaints received	38
Figure 3	Evolution of the number of complaints, including admissible complaints, received by the EDPS	39
Figure 4	Europol statistics	47
Figure 5	Number of personal data breach notifications per month	52
Figure 6	Number of personal data breach notifications per month for the years 2019 and 2020	53
Figure 7	Type of submission on personal data breach notifications in the year 2019 and 2020	53
Figure 8	Type of data breach notifications	54
Figure 9	Root cause of the personal data breach incidents	54
Figure 10	Root cause of the personal data breach incidents - Comparison 2019-2020	55
Figure 11	Number of individuals affected from personal data breach incidents	55
Figure 12	Number of personal data breach where the controller informed the data subject	56
Figure 13	Special categories of data in personal data breach incidents	56
Figure 14	Social media statistics	76



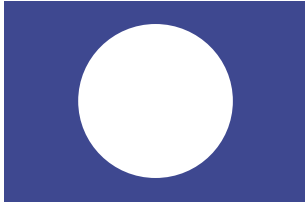
# ABBREVIATIONS

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

## ABBREVIATIONS

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





## GLOSSARY

The glossary is available on the [EDPS website](#)

<b>Accountability</b>	Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice.
<b>Adequacy decision</b>	A decision adopted by the European Commission that a non-EU country ensures an adequate level of protection of personal data.
<b>Artificial Intelligence (AI)</b>	Enables computers and machines to mimic the perception, learning, problem-solving and decision-making capabilities of the human mind.
<b>Biometrics</b>	Methods for uniquely recognising data subjects based upon one or more intrinsic physical or behavioural traits.
<b>Charter of Fundamental Rights of the EU</b>	Sets out the civil, political, economic and social rights of EU citizens and residents.
<b>Confidentiality</b>	Duty not to disclose personal data to unauthorised individuals.
<b>Consent</b>	Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice.
<b>Contact tracing</b>	Process to identify individuals who have been in contact with those infected by disease, such as COVID-19.
<b>Convention for the Protection of Individuals with regard to automatic processing of personal data (Convention 108)</b>	Adopted in 1981, it is the first legally binding international instrument in the field of data protection.
<b>Court of Justice of the European Union (CJEU)</b>	Ensures uniform interpretation and application of EU law in EU Member States. Ensures that EU Member States and EUIs abide by EU law.

## GLOSSARY

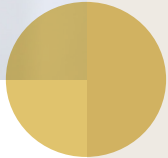
<b>Data controller</b>	Party that, alone or jointly with others, determines the purposes and means of the processing of personal data.
<b>Data minimisation</b>	The principle of “data minimisation” means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose.
<b>Data processor</b>	Party that processes personal data strictly on behalf of the data controller.
<b>Data protection authority (DPA)</b>	An independent supervisory body monitoring the processing of personal data, providing advice and adjudicating complaints, within its jurisdiction.
<b>Data protection by default</b>	Data protection should be incorporated by default into any system, service, product or process.
<b>Data protection by design</b>	Privacy by design aims at building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principle.
<b>Data Protection Impact Assessment (DPIA)</b>	The DPIA tool process aims at providing assurance that controllers adequately address privacy and data protection risks of ‘risky’ processing operations. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of ‘data protection by design’ where it is needed the most, i.e. for ‘risky’ processing operations.
<b>Data Protection Officer (DPO)</b>	An expert on data protection law and practices, who operates independently within an organisation to ensure the internal application of data protection.
<b>Data subject</b>	The person whose personal data is processed.
<b>Data transfer</b>	Transfer of data outside the EU / European Economic Area (EEA).
<b>Derogations</b>	Provisions permitting EU Member States to exercise a degree of discretion over how certain provisions of the General Data Protection Regulation (GDPR) will apply.
<b>European Data Protection Board (EDPB)</b>	Independent European body which contributes to the consistent application of data protection rules throughout the European Economic Area (EEA), and promotes cooperation between the EEA’s data protection authorities.

<b>E-privacy Directive</b>	Sets out rules for the processing of personal data and the protection of privacy in the electronic communications sector. The E-privacy directive is also known as Directive 2009/136/EC.
<b>European Asylum Dactyloscopy Database (EURODAC)</b>	EU database that identifies asylum seekers applying for international protection by collecting their fingerprint data.
<b>European Commission</b>	Shapes the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget.
<b>European Economic Area (EEA)</b>	EU Member States and Iceland, Liechtenstein and Norway.
<b>European Parliament</b>	Members directly elected in EU Member States to represent people's interests in regard to EU law-making and to make sure other EUs are working democratically.
<b>European Union (EU)</b>	An economic and political union between <u>27 European countries</u> .
<b>General Data Protection Regulation (GDPR)</b>	Sets out rules on the rights of data subjects, the duties of data controllers and processors processing personal data, international data transfers and the powers of data protection authorities.
<b>Large-scale IT systems</b>	Several databases created or about to be created by the EU can be considered large by various measures: number of people using the system for different purposes, amount of data collected, stored, accessed, manipulated, number of connections between components, etc.
<b>Law Enforcement Directive</b>	Sets out rules for the processing of personal data by data controllers for law enforcement purposes. The LED is also known as Directive (EU) 2016/680.
<b>Personal data</b>	Any information relating to an identified or identifiable data subject.
<b>Privacy Enhancing Technologies (PETs)</b>	Coherent system of ICT measures that protect privacy.
<b>Processing</b>	Any operations performed on personal data such as collection, recording, storage, alteration, retrieval, use, disclosure, restriction or erasure.
<b>Regulation (EU) 2018/1725</b>	Lays down the data protection obligations for the EU institutions and bodies when they process personal data and develop new policies.
<b>Right of access</b>	Right of any data subject to obtain confirmation that their personal data is being processed and why.

## GLOSSARY

<b>Right to erasure</b>	Right of any data subject to have their personal data erased.
<b>Right of information</b>	Right of any data subject to know that their personal data is processed and for what purpose.
<b>Right of rectification</b>	Right of any data subject to obtain the rectification of their personal data without delay where inaccurate or incomplete.
<b>Right to object</b>	Right of any data subject to object to the processing of their personal data.
<b>Schengen Information System (SIS II)</b>	Records personal data of non-EU country nationals who are banned from entry to Schengen territory, people wanted in relation to criminal proceedings or under police surveillance and missing people.
<b>“Schrems II” Judgment</b>	CJEU ruling invalidating EU-US Privacy Shield and confirming the validity of Standard Contractual Clauses.
<b>Special category data</b>	Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data.
<b>Standard Contractual Clauses (SCCs)</b>	Provide adequate safeguards for data transfers from the EU or the EEA to non-EU countries.
<b>Support Pool of Experts (SPE)</b>	Support investigations and enforcement activities of significant common interest for the EDPB.
<b>Third country</b>	A country outside the EU, not bound by the GDPR, but may be recognised as offering an adequate level of protection for personal data in order to enable data transfers.
<b>Third party</b>	A party other than the data controller, processor or data subject. In the context of EUIs this may be a public authority or private party which temporarily needs to process the personal data of an official.
<b>Transfer Impact Assessment (TIA)</b>	Identifies whether the non EU country of destination provides a level of data protection essentially equivalent to the one afforded under EU law.





## FOREWORD

2020 was a challenging year, a year none of us were expecting.

The pandemic has not only dramatically changed the way we live and work; it has also brought at the centre of public debate the role and nature of our fundamental rights, including the rights to privacy and data protection.

With the pandemic came a new reality. From the perspective of a data protection authority, it was first and foremost a test. It was a challenge to ensure compliance in the ever-growing digitalised world and to provide timely advice to authorities, controllers and citizens on the data protection aspects of measures taken due to the pandemic.

The EDPS answered promptly to this task, having established an internal COVID-19 taskforce, composed of members of all the EDPS' units and sectors, to coordinate and proactively undertake actions related to the interplay between privacy and the pandemic. Believing in the EDPS' specific role in the EU institutional landscape, we called for a pan-European approach to combat the virus, in particular in the context of contact tracing apps.

With the teleworking regime, the EDPS had to adjust its approach when it came to carrying out its core activities. We took this as an opportunity to engage in an even closer dialogue with stakeholders, including public authorities, civil society and academia. We continued to be active in the field of investigations. Among others, we concluded the inquiry into the use of large datasets by Europol and we issued our findings and recommendations following an investigation into EULs' use of Microsoft products and services, which we presented at the second meeting of the Hague Forum.

The “Schrems II” Judgement, a landmark decision of the Court of Justice of the European Union (CJEU), has contributed to what has already been a particularly eventful year for a data protection authority. The EDPS has actively participated in, and contributed to, the EDPB’s work resulting from the judgement, particularly regarding the measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. At the same time, we prepared our own strategy aimed at ensuring the compliance of EUIs with the CJEU’s Judgement.

Looking ahead, in June 2020, we presented the EDPS strategy for 2020-2024 ‘Shaping a Safer Digital Future’, based on Foresight, Action and Solidarity. In this spirit, the EDPS proposed, among other initiatives, the Support Pool of Experts which aims to bring together the EDPB members’ efforts to address the need for a stronger enforcement of EU data protection laws.

We continued to act as a trusted advisor to the European Commission, the Council and the European Parliament on the many legislative and non-legislative proposals or other initiatives affecting the rights to privacy and data protection. This included, for example, our Opinions on the European strategy for data, on Artificial Intelligence or the proposed temporary derogations from the e-privacy framework. We also offered our expertise to the legislator with our own-initiative Opinions on the use of data for scientific research and health-related purposes, to name a few.

We have further developed our monitoring-related activities, analysing and acting as a reference point for clarifying technological issues related to privacy and data protection.

It is with particular satisfaction that I present this document: the summary and overview of everything we have done during these difficult months. The Annual Report 2020 shows the resilience, dedication and hard work of the EDPS staff to whom I would like to offer my heartfelt thanks.



**Wojciech Wiewiórowski**  
European Data Protection Supervisor



# MISSION, VALUES AND PRINCIPLES

The work of the [European Data Protection Supervisor \(EDPS\)](#) is guided by its mission. The EDPS' 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 the EDPS' 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 the EDPS' 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 with 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.





# 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 amid 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.

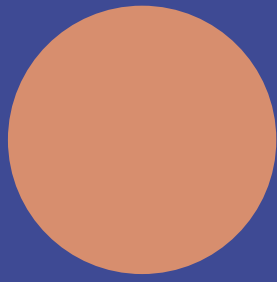
There are three core pillars to the EDPS strategy, which outline the guiding actions and objectives for the organisation from 2020 to the end of 2024.

**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.

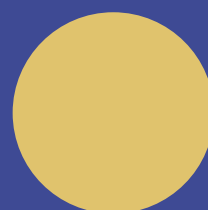
**Action:** the EDPS proactively develops tools for EU institutions to be world leaders in data protection. We aim to promote coherence in the activities of enforcement bodies in the EU with a stronger expression of genuine European solidarity, burden-sharing and a common approach.

**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.





2020  
2024



001000111110  
00100110111000001100  
0010011110011001110010000  
11100101010100100000000010  
0010000011000100010101110000111  
0010100110001000110110100100011101  
101111001010111010010100000100100010  
101101011010110111110101011001010101  
010001010010101010000011010111000010100  
11101110011010110001111000001100100000101  
010000011000011111111101111000110100011000  
000101010001100110110001010110000100111001  
10010010011010100100110110001000010010  
0111010110001101000110011100001100111000100101  
011010110011010000010010110101111001010000011  
100111010101101001101101111000100001100110  
1011000100000010100111101101110111000010101101  
00111001010010111010111100011111101101001111000  
110011001001101000101000000000101110101010010011  
110100111110111101010000011010001101100010010111  
10000111111010101110111001100010100000100110000  
111010011011011110001000110010011001110101110111  
0010110010010000001110110100000101011100  
000001001100110010110011110011111011  
001101110011001100111000101000001000001  
10011100111001000001000101000100100000  
0101011100000101110001010111011100  
10010001100110011110111000001110  
01101001000110110111001010010000000101  
0100000100110000010011010000101011100011  
0101011001010101010001011000110110111111111  
1010111100001010010000010000111101100101111  
10011111010011001011001111001111101110111  
1000110011010111000101000001000001111110  
01000001000001000101000100100000101001  
001010000101110001010111011100110100  
11010110011111101110000001110001110  
01101110010100100000000101011010  
0011010000101011100011111111  
00011011011111111111100101  
1101100101111110101  
110010110011

## 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.

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.

### 1.1 Supervision and Enforcement

In its role as the DPA of EUIs, the EDPS aims 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 the EDPS 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.

### 1.2 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 the form of:

**Opinions:** our Opinions are issued in response to mandatory requests by the Commission which is legally obliged to seek our guidance on any legislative proposal, or draft IA/DA, 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.

## ABOUT THE EDPS

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 Commission and are addressed to the EU co-legislator.

**Formal Comments:** similar to our Opinions, our Formal Comments are issued in response to a request from the 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.

**Informal Comments:** the European Commission is encouraged to consult the EDPS informally before adopting a proposal which has an impact on data protection. This allows us to provide the 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 Commission may also consult the EDPB. In such cases, the EDPS and EDPB work together to issue a joint opinion.

Beyond mandatory legislative consultations, the EDPS also has 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, the EDPS has been organising workshops on data protection with International Organisations, since 2005. For its 9th edition, the International

Organisations workshop took place via videoconference in October 2020. The EDPS is also an active member of the Global Privacy Assembly ([see section 3.8: 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.



## 1.3 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 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 ubiquitous use of Artificial Intelligence (AI) across private and public sectors, such as in healthcare and law enforcement, which involves the processing of individuals' personal data that may have a significant impact on their fundamental rights (including the right to data protection). As such, the EDPS units brought together their various expertise as our AI task force to provide appropriate guidance and advice to all EUIs on various AI initiatives, such as the EDPS [Opinion on the European Commission's White Paper on Artificial Intelligence](#) and the [Opinion on the European Data Strategy](#);
- our participation in the EDPB task force established following the "[Schrems II](#)" ruling;
- our [Online Workshop: Data Protection within International Organisations 2020](#), which led to the establishment of a task force through which the EDPS further promotes EU data protection standards internationally; and
- a variety of EDPS [Opinions](#) and other data protection work in the field of Justice and Home Affairs, such as the preparation of the EDPS [Opinion on Europol's mandate review](#).

### 1.4 The EDPS work on transversal issues

The EDPS brings together experts with different backgrounds and perspectives. Together we are able to respond creatively to data protection challenges and find solutions that benefit society as a whole, including the most vulnerable.

The EDPS Policy & Consultation (P&C), Supervision & Enforcement (S&E) and Technology & Privacy (T&P) units worked together on various initiatives in 2020, and will continue to do so in 2021.

The following list, although not exhaustive, includes examples of such collaboration on transversal issues:

- our COVID-19 task force, including initiatives such as our [Orientations from the EDPS: Reactions of EUIs as employers to the COVID-19 crisis](#) which compiles advice on individuals' right to data protection, health data and teleworking for data controllers and DPOs in the EUIs, and [EDPS Comments on cross-border exchange of data between national COVID-19 contact tracing and warning mobile applications](#);





# THE EDPS' 2020 HIGHLIGHTS

## An overview of 2020

The year 2020 was unique for the world and, by extension, for the European Data Protection Supervisor (EDPS). Like many other organisations, the EDPS had to adapt its working methods as an employer, but also its work since the COVID-19 health crisis strengthened the call for the protection of individuals' privacy, with the appearance of contact tracing apps and other technologies used for the fight against COVID-19. While technology can certainly contribute to limiting the spread of COVID-19, our priority remains to ensure that individuals' personal data and right to privacy is protected.

2020 also marked new beginnings for the EDPS. On 30 June 2020, we presented our [Strategy 2020-2024](#). The Strategy's overarching aim is to shape a safer digital future, with three core pillars outlining the guiding actions and objectives for the EDPS to the end of 2024: **Foresight, Action and Solidarity**.

These three pillars, and our Strategy as a whole, were the driving force for our work in 2020.

## 2.1 Data protection in a global health crisis

The COVID-19 pandemic has taught us that privacy, like any other fundamental right, is nothing without

solidarity. With this in mind, we have worked closely within the EDPS and with the European Data Protection Board (EDPB), the data protection officers (DPOs) of EU institutions, bodies, offices and agencies (EUIs), as well as with other European and international privacy and technology experts, to protect individuals and their personal data.

Our first initiative in this context was to immediately establish an internal [task force](#) to actively monitor and assess governmental and private sector responses to the COVID-19 pandemic. Throughout 2020, the COVID-19 task force has followed and anticipated future developments with an impact on data protection and privacy, allowing the EDPS to serve as a catalyst for a privacy-driven response and as a point of reference for stakeholders across and beyond Europe.

As the EU data protection authority of EUIs, we supported EUIs in their effort to safeguard their employees' health in a privacy-compliant way by issuing our Orientations on [body temperature checks](#), [manual contact tracing](#), and [reactions of EUIs as employers](#).

We also took on an active role at regional and international level with our participation and leadership in international fora such as the Global Privacy Assembly (GPA) (formerly the International Conference of Data Protection and Privacy Commissioners) and other conferences. In particular,



we engaged with experts from the public health community in the European Union (EU) and other international organisations to better understand the needs for epidemiological surveillance and to accurately measure the efficiency and purpose of the tools being developed with regard to personal data protection, for example, by developing together practical guidance on data protection by design ([see section 3.1](#)).

## 2.2 EUIs' compliance with data protection law

### Providing the necessary tools for EUIs

As the data protection authority for EUIs, the EDPS provides them with the necessary tools to comply with [Regulation \(EU\) 2018/1725](#).

We have achieved this during 2020 through various initiatives, ranging from issuing strategic documents and publishing our investigations, to reinforcing our collaboration with the data protection officers of the EUIs by providing training to raise their awareness of data protection issues and their responsibilities.

The EDPS used existing, and developed new, tools and promoted a coherent approach to the application of data protection during 2020 in order to support EUIs to continue to lead by example in safeguarding digital rights and responsible data processing, according to the **Action and Foresight** pillars of our Strategy 2020-2024.

We have advised and guided EUIs with regard to tools, such as Data Protection Impact Assessments (DPIAs), and provided relevant training in order to share knowledge, expertise and contribute to the smart administration of the EUI environment. We have utilised a range of methods, such as our 'DPIA in a nutshell' [Factsheet](#), a [Report](#) on how EUIs carry out DPIAs which contains lessons learned and best practices observed by the EUIs, a survey to determine specifically how EUIs have been using DPIAs and a [video](#) on the same subject for DPOs. We also continue to regularly update our Wiki, a resource created in November 2019 for data protection officers and data protection coordinators to help them comply with Regulation (EU) 2018/1725. We

have also been working on developing version 1.0 of the [Website Evidence Collector](#) to help DPAs, data controllers, data protection practitioners and web developers to help them ensure that their websites are compliant with the General Data Protection Regulation (GDPR) and Regulation (EU) 2018/1725.

### Supervising the Area of Freedom Security and Justice

We launched our supervision of the EU agency for judicial cooperation, [Eurojust](#) (12 December 2019) and are increasing the supervision of the [European Public Prosecutor's Office's](#) (EPPO) data protection-related activities.

On 5 October 2020, we rendered public our [inquiry](#) on the EU Agency for Law Enforcement Cooperation's ([Europol](#)) big data challenge, namely Europol's processing of large datasets received from EU Member States and other operational partners, or collected in the context of open source intelligence activities. We found that the processing did not comply with the provisions of [Regulation 2016/794](#), in particular with the principle of data minimisation. We admonished Europol to implement all necessary and appropriate measures to mitigate the risks for individuals' data created by the processing of large datasets ([see section 3.4](#)).

### The Hague Forum

On 2 July 2020, The Hague Forum, co-established by the EDPS, met for the second time, bringing together EUIs and other international organisations to exchange information and strengthen their negotiation power with ICT service providers, including cloud service and communications providers. On this occasion, we issued a [Public Paper](#) detailing our findings and recommendations on the use of Microsoft products and services by EUIs, in which we emphasise that, when EUIs enter into contractual relationships with IT service providers, the terms of these contracts should reinforce the EUIs control over how and why personal data is processed ([see section 3.2.2](#)).

### Compliance with “Schrems II” ruling

The EDPS issued its [Strategy for EUIs to comply with the ‘Schrems II’ ruling](#) following the [judgment](#) of the Court of Justice of the European Union on 16 July 2020. The judgement reaffirms, among other issues, the importance of maintaining a high level of protection of personal data transferred from the European Union to non-EU countries. The EDPS strategy includes a roadmap of actions for EUIs to ensure that ongoing and future international transfers are carried out in accordance with EU data protection law.

## 2.3 Safeguarding digital rights

The overarching objective of the EDPS is to promote a safer digital future for the EU. Our work on legislative consultations is instrumental to achieving this objective.

The EDPS promotes a positive vision of digitisation that enables us to value and respect all individuals, as per the Solidarity pillar of our Strategy 2020-2024. Therefore, we issue and address [Opinions](#) and recommendations to the EU legislators on the impact that their initiatives may have on individuals and their right to data protection to ensure that they promote digital justice and privacy for all within their initiatives.

The EDPS is also interested in policy initiatives to promote ‘digital sovereignty’ to help ensure that data generated in Europe is processed in accordance with European values. At the same time, we are committed to help overcome the detrimental vendor’s lock-in syndrome in the EUIs ([see section 3.2.2](#)).

### Opinion on a new EU-UK partnership

On 24 February 2020, the EDPS issued an [Opinion](#) on the opening of negotiations for a new partnership with the United Kingdom (UK). The EDPS supports a partnership which affirms the EU and UK commitment to and respect for a high level of data protection and the EU data protection rules. In its Opinion, the EDPS makes recommendations regarding commitments to respect fundamental

rights (including data protection) equivalent to those for the economy and security, defining priorities for international cooperation other than law enforcement particularly between public authorities (including EUIs) and assessing transfers of personal data in the light of the CJEU [Opinion 1/15](#) for the economic and security partnerships ([see section 3.6.2](#)).

### Opinion on the European strategy for data

The EDPS adopted an [Opinion](#) on 16 June 2020 to emphasise that the European strategy for data should stay true to European values, in particular respect for the fundamental rights of individuals such as the right to data protection ([see section 3.2.4](#)).

### Opinion on combatting child abuse online

On 10 November 2020, the EDPS issued an [Opinion](#) on a proposal for temporary derogations from the ePrivacy directive for the purpose of combatting child sexual abuse online. In its Opinion, the EDPS stresses that measures to detect, remove and report child abuse must be accompanied by a comprehensive legal framework which meets the requirements of [Articles 7](#) and [8](#) of the Charter of Fundamental Rights of the EU. Moreover, in order to satisfy the requirement of proportionality, the legislation must set clear and precise rules governing the scope and application of the relevant measures and imposing minimum safeguards to provide sufficient guarantees of the protection of personal data against the risk of abuse ([see section 3.6.4](#)).

### Opinion on the New Pact on Migration and Asylum

On 30 November 2020, the EDPS issued an [Opinion](#) on the New Pact on Migration and Asylum to ensure that the proposal for more effective management of asylum and immigration incorporates a DPIA to help identify and address the relevant data protection implications ([see section 3.6.5](#)).

### Opinion on the European Health Data Space

The EDPS published a [Preliminary Opinion](#) on 17 November 2020 on the [European Health Data Space](#) (EHDS), to ensure that this platform for exchanging health data and fostering medical and scientific research prioritises the protection of individuals' personal data within its development ([see section 3.2.4](#)).

## 2.4 Monitoring technologies

The EDPS aims to be a recognised and respected centre of expertise that helps understand the impact of the design, deployment and evolution of digital technology upon the fundamental rights to privacy and data protection, and accordingly we have included this in the Foresight pillar of our Strategy 2020-2024. Therefore, we placed strategic importance during 2020 and for the foreseeable future upon integrating the technological dimension of data protection into our work. As a DPA, we also continue to closely examine the potential risks and opportunities offered by technological advances, seek to understand the possible benefits of new technologies and encourage the integration of data protection by design and data protection by default in the innovation process.

Examples include, but are not limited to, our contribution during 2020 to developing strong oversight, audit and assessment capabilities for technologies and tools that are increasingly 'endemic' to our digital ecosystem, such as artificial intelligence and facial recognition ([see section 3.5.3](#)).

### TechDispatch

The EDPS also continued to build upon existing initiatives such as our [TechDispatch](#) reports, launched in July 2019, for the EDPS to contribute to the ongoing discussion on new technologies and data protection. Focusing on a different emerging technology each issue, we aim to provide information on the technology itself, an assessment of its possible impact on privacy and data protection and links to further reading on the topic ([see section 3.5.1](#)).

### Internet Privacy Engineering Network

The EDPS has also continued to organise sessions and workshops (albeit virtually) of the [Internet Privacy Engineering Network](#) (IPEN), which we founded in 2014, to allow us to bridge the gap between legal experts and engineers when implementing data protection safeguards and monitor the state of the art of privacy enhancing technologies. With this endeavour, we continue to develop core knowledge about how essential and emerging technologies work for privacy and data protection by exchanging views academia and innovators in the private sector, among other relevant actors ([see section 3.5.3](#)).

## 2.5 The EDPS as a member of the EDPB

The EDPS believes that a strong expression of genuine European solidarity, burden sharing and common approach is necessary to ensure the enforcement of data protection rules. We strongly believe in this and have included this in our **Action** pillar of the Strategy 2020-2024.

As an example of how we put this conviction into practice, the EDPS, as a member of the EDPB, works closely with other DPAs for the consistent application of data protection laws across the EU ([see section 3.6](#)).

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

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

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

### 2.6 International cooperation in data protection

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. In 2020, the EDPS has continued to dedicate substantial time in promoting global data protection convergence and cross-border dialogue. Despite the pandemic-related challenges, we have continued to exchange best practices and information with international organisations and interlocutors outside Europe, as well as developing European and international cooperation measures, and promoting joint enforcement actions and active mutual assistance.

In 2020, we have pursued this objective via fora, such as the GPA; the Computers, Privacy and Data Protection Conference (CPDP) and international organisations workshops, addressing the data protection challenges arising – among others – with the use of new technologies, within the fight against COVID-19 and in law enforcement ([see section 3.8](#)).

### 2.7 Internal administration

The EDPS Human Resources, Budget and Administration Unit (HRBA) has provided support throughout 2020 to ensure that both the EDPS Management and operational teams have the financial, human and administrative resources and tools to achieve the goals set out in our Strategy 2020-2024.

In light of the COVID-19 pandemic, the HRBA has had to adapt its organisation during 2020 to ensure business continuity, by developing an innovative action plan to enhance the functioning of the EDPS and the wellbeing of its staff, in particular preparing the workforce for teleworking.

The EDPS continued to grow in 2020, both in terms of financial and human resources. This required agility, flexibility and creativity on the part of HRBA, particularly given the exceptionally difficult context of the COVID-19 pandemic.

HRBA introduced new initiatives in 2020 to

enhance the well-being of EDPS staff – such as internal coaching and other support activities – and will continue to pursue these endeavours in 2021. This ensures that we remain a socially responsible organisation and manifests our belief that staff with higher levels of well-being learn and work more effectively, are more creative, have better relationships, are more social in their behaviour, and ultimately feel more satisfied with their working life ([see section 5.2](#)).

### 2.8 Communicating data protection

Public interest in, and engagement with, data protection and the work of DPAs only continues to grow. This has and continues to be even more the case in light of the COVID-19 pandemic, which has increased the acceleration of the digitalisation of individuals' daily lives. People feel more aware of and concerned about their digital footprint and the importance of protecting their personal data.

During the COVID-19 pandemic, it has been of particular importance to adapt and continue to strengthen the EDPS' online presence in order to fully connect with the relevant audience and stakeholders. The EDPS Information and Communication Team has achieved this objective using a variety of methods, in particular via EDPS blogposts, social media campaigns and monthly newsletters.

The Team's efforts focused on other objectives as well, in particular promoting the EDPS Strategy 2020-2024 and developing a new visual identity for the EDPS ([see section 5.1](#)).

### 2.9 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 2020. These results are measured against initial targets, or against the results of the previous year, used as an indicator.

The outbreak of the COVID-19 pandemic, and its far-reaching consequences at every level, substantially changed the context and circumstances in which the EDPS had to operate. Therefore, the KPIs monitoring this year's results should be read with this context in mind.

In 2020, we met or surpassed - in some cases significantly - the targets set in five out of eight KPIs. This includes, **KPI 1** on the number of initiatives related to our technology and privacy work; **KPI 2** measuring the number of activities on cross-disciplinary actions; **KPI 3** concerning the number of cases dealt with at international level; **KPI 4** on the number of Opinions and Comments issued in 2020; as well as **KPI 6** demonstrating an increase of our followers on our social media platforms.

**KPI 5**, measuring EUIs level of satisfaction on guidance and training received in 2020 was not assessed; the vast majority of training and meetings were conducted remotely, and satisfaction surveys were not conducted due to the technical limitations that could not allow us to ensure anonymous feedback. The small number of in-person sessions that took place in 2020 are not sufficiently representative to draw meaningful conclusions; as a result, this KPI has not been assessed in 2020.

**KPI 7** reflects the outcome of the periodic staff satisfaction survey, which occurs every two years. The survey was launched in June 2020, three months after the beginning of the COVID-19 crisis amid a climate of anxiety and uncertainty. These extraordinary circumstances may, in part, explain why we failed to reach the set target. In addition, the participation rate was rather low (45%) and there were quite a lot of newcomers for whom it may have been difficult to answer some of the questions in the survey.

**KPI 8** on budget implementation shows that, in 2020, 72.97% of the EDPS's allocated budget was implemented, a substantially lower figure compared to 2019's budget implementation figure of 92% and well below the 90% target. This is mainly due to the

COVID-19 pandemic which dramatically affected the activities of the EDPS. When the Belgian government declared the first lockdown in March 2020, severe (ongoing) restrictions were enforced on the movement of staff and other individuals. This directly impacted the missions' expenses and experts' reimbursements expenses which constitute a major part of the budget. Other budget items were indirectly affected as well (e.g. the interpretation expenses). There were some other external factors which also impacted budget execution to a lesser extent (delays in the availability of offices in the Montoyer 30 building and postponement of the related works). We expect that the pandemic will also have a substantial impact on the year 2021 as travel restrictions are expected to continue until the vaccination campaign is in its advanced stage.



## THE EDPS' 2020 HIGHLIGHTS

KEY PERFORMANCE INDICATORS		Results on 31.12.2020	Target 2020
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 EDPS	9 initiatives	9 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 at international level (EDPB, CoE, OECD, GPEN, International Conferences) for which EDPS has provided a substantial written contribution	42 cases	10 cases
KPI 4 External Indicator	Number of Opinions/Comments issued in response to consultation requests (COM, EP, Council, DPAs...)	6 Opinions 25 Formal Comments	10 Opinions/ Comments
KPI 5 External Indicator	Level of satisfaction of DPO's/DPC's/ controllers on cooperation with EDPS and guidance, including satisfaction of data subjects as to training	/	70%
KPI 6 External Indicator	Number of followers on the EDPS social media accounts	62970 (LI: 38400, T:22493, YT: 2077)	Previous year's results + 10%
KPI 7 Internal Indicator	Level of Staff satisfaction	71%	75%
KPI 8 Internal Indicator	Budget implementation	72,97 %	90%

Figure 1. EDPS KPI analysis table in 2020





## 2020 — AN OVERVIEW

### 3.1 Data Protection amid a global health crisis

Following the outbreak of the COVID-19 pandemic, the European Data Protection Supervisor (EDPS) immediately established an internal [task force](#) to actively monitor and assess governmental and private responses to the outbreak. Throughout 2020, the COVID-19 task force has been following developments and preparing for the future of data protection and privacy after the COVID-19 crisis.

From the outset, [the EDPS emphasised](#) the need for a pan-European approach in tackling the pandemic. In addition to providing guidance to EU institutions, bodies and agencies (EUIs), the EDPS closely cooperates with other members of the [European Data Protection Board](#) (EDPB) to offer practical guidance in relation to the most pressing challenges of the pandemic. Throughout its guidance, the EDPS stresses that pandemic-related technologies requiring the processing of personal data must be temporary, have a defined and limited purpose, and comply with EU data protection law.

*As we discuss digital solutions to manage the pandemic, and we subject them to public and democratic debate, we shall keep sight of the endemic problems of the digital ecosystem and have them subject to democratic oversight and deliberations.*  
– [Wojciech Wiewiórowski](#)

#### 3.1.1 Contact Tracing Apps and monitoring the spread of the pandemic

Contact tracing can be a useful tool to reduce the rate of infection of COVID-19 by breaking the chain of transmission; it can be performed manually or with technological support, including mobile apps.

In efforts to help mitigate the implications of the virus, the EDPS took leadership in assessing data protection standards in a number of initiatives:

- **The Apple & Google Framework** – the EDPS analysed Google and Apple's joint effort to develop Bluetooth-based technologies to help health authorities reduce the spread of the virus and stressed the importance of ensuring interoperability between operating systems. The EDPS' technical assessment contributed to wider efforts to evaluate the Joint Exposure Notification system and to promote privacy-preserving contact tracing.
- **IPEN Webinar on contact tracing apps** – In the context of its mission to promote the understanding of privacy enabling technologies among technical experts, the Internet Privacy Engineering Network ([IPEN](#)) organised the webinar on [Contact Tracing Apps as a large-scale exercise in privacy engineering](#). The webinar explored how privacy engineering has found



its place in the development of contact tracing apps, and whether the promoted approach has affected the state of the art in data protection by design and by default.

- **TechDispatch #1/2020: Contact Tracing with Mobile Applications** – As part of a wider EDPS campaign on monitoring emerging developments in technology, this TechDispatch summarises key concepts and concerns on contact tracing apps, based on their data protection implications.
- **EDPB Membership** – The EDPS took an active role in the development of both the [EDPB guidance on the use of location data and contact tracing applications](#) and the [EDPB guidance on the use of health data for the purpose of scientific research purposes](#).
- **Consultations** – The EDPS was consulted by various EUIs, including the European Commission, on the data protection implications of monitoring the spread of the pandemic, e.g. using location data.
- **Conference participation** – European Data Protection Supervisor Wojciech Wiewiórowski and EDPS staff attended a number of conferences at European and Member State level to exchange views with authorities, EUIs and data protection experts. These conferences fuelled discussions on EU-wide solutions in the fight against the pandemic that promote a data protection culture and legal compliance.

### 3.1.2 Supporting EUIs as employers

The EDPS spent the initial months of the pandemic monitoring and ensuring the lawful processing of personal data by EUIs, as they not only had to respond to the crisis within their policy roles, but also as employers. In the face of new challenges, such as the transition towards remote working, the EDPS worked closely with the data protection officers (DPOs) of EUIs to provide helpful guidelines and best practices for ongoing compliance.

In March 2020, the EDPS issued guidance to all EUIs on how to answer to national public health

authorities' requests to disclose information, including personal data. The EDPS recommends that data protection authorities of EUIs promote data protection principles and culture internally, reminding management of the remit of their roles in the pursuit of precautionary measures.

In July 2020, the EDPS published the document [Orientations from the EDPS: Reactions of EU institutions as employers to the COVID-19 crisis](#) with the aim to guide EUIs on appropriate practices regarding teleworking tools, staff management, health data aspects and replying to data subject access requests. The EDPS reiterates that data protection rules do not hinder the business continuity of EUIs' operations, and that controllers and DPOs of EUIs should work together to develop adequate organisational responses to the crisis.

In December 2020, the EDPS conducted a survey among EUIs aiming to investigate new processing operations, IT tools and solutions implemented during the pandemic. The purpose of this survey was to identify new topics requiring specific orientations from the EDPS and to ensure that newly employed measures are compliant with data protection requirements.

### 3.1.3 EDPS Orientations on the use of manual contact tracing by EUIs

In 2020, the EDPS worked on orientations, which will be published in 2021, related to manual contact tracing systems implemented by EUIs in order to trace individuals who have been in close contact with a person infected with COVID-19.

The EDPS considers that manual contact tracing is compatible with the requirements of Regulation (EU) 2018/1725 as long as EUIs put in place comprehensive data protection measures. The ethics of public health information require that privacy considerations are thoroughly addressed at all levels of contact tracing activities.

In its Orientations, the EDPS distinguishes between the processing of health data of EUIs' staff members and non-staff members who are visiting the EUIs'

premises.

In view of the high sensitivity of the data at stake and the high risk for the privacy of individuals, EUIs need to conduct a DPIA when developing and putting in place a manual contact tracing operation. By performing a DPIA, controllers will be able to design a robust and data protection-compliant system that will contribute to the smooth deployment of such system and its operational success.

Informing affected individuals should be done on the basis of a clear protocol. This means limiting the amount of personal information (i.e. personal data) given to individuals to what is considered as strictly necessary for contact-tracing purposes. Additionally, adequate security measures need to be put in place when information and communication technologies are used for this purpose. The EUI shall take steps to ensure that any person acting under its authority process the data under its specific instructions.

### 3.1.4 EDPS guidelines on body temperature checks

A number of EUIs have implemented body temperature checks upon entry to their premises as a strategy to prevent the virus from spreading in the workplace and to enable the return to workplace. Given that the systematic check of the body temperature of staff and other visitors may constitute an interference with individuals' rights to private life and data protection, the EDPS carefully assessed this practice to ensure that it aligns with EU data protection law.

In its [Orientations](#), the EDPS distinguishes between "basic body temperature checks" (i.e. checks which are not followed by registration, documentation or other processing of individuals' personal data) and other systems of temperature checks, combined with identity verification. The EDPS argued that basic body temperature checks would only be subject to legality, necessity and proportionality considerations derived from the Charter of Fundamental Rights of the European Union, while other systems of temperature checks would, instead, be fully subject to the data protection regime of Regulation (EU) 2018/1725.



In this context, as for any data processing operation, the obligations of data protection by design and by default should be applied to ensure that data collection in the context of body temperature checks is minimised. While additional data protection safeguards must be put in place - depending on the processing capability of the adopted system used to carry out body temperature checks - the highest standards of transparency towards individuals should be put in place irrespectively of the type of system used. Finally, the EDPS advises EUIs implementing temperature checks to continuously review the necessity and proportionality of such measures in light of the evolution of the epidemiological situation and its scientific understanding.

### 3.1.5 The Global Privacy Assembly resolutions on COVID-19

As one of its active members, the EDPS took part in the [GPA](#) activities related to the pandemic.

In particular, the EDPS sponsored the [Resolution on the Privacy and Data Protection Challenges arising from the COVID-19 Pandemic](#), which praises national DPAs for their proactive contributions to the creation and dissemination of best practices; encourages all members and observers to promote cooperation with non-privacy regulatory authorities; and reminds of the need to adopt a privacy-by-design approach when deploying contact tracing initiatives. Furthermore, the Resolution encourages all members and partners to engage in further awareness-raising and collective-capacity-building initiatives, including webinars and workshops. With this resolution, a new temporary Working Group

on COVID-19 related privacy and data protection issues was established.

## 3.2 Safeguarding EU digital rights

In 2020, as a result of the COVID-19 pandemic, individuals spent more time at home than ever before, further increasing their online presence, leading to increased amounts of personal data circulating digitally. The EU data protection regime is a solid basis for a human-centric digital life where individuals remain in control of their personal data. In this context, the EDPS continues to lead by example in safeguarding digital rights and responsible data processing, working towards the achievement of ‘digital sovereignty’, as outlined in the [EDPS Strategy 2020-2024](#).

### 3.2.1 Strategy for EUIs to comply with the “Schrems II” ruling

On 16 July 2020, the Court of Justice of the European Union issued a judgement in case C-311/18, so-called “[Schrems II](#)” ruling, in which it invalidated the EU-US Privacy Shield, a personal data transfer mechanism.

The EDPS recognised the impact of the judgement and the role of DPAs in ensuring that the decision is complied with. Therefore, on 29 October 2020, the EDPS issued its [Strategy for Union institutions, offices, bodies and agencies to comply with the “Schrems II” ruling](#) aiming to monitor compliance of these bodies with the ruling, and to ensure that ongoing and future international transfers are carried out in accordance with EU data protection law. The EDPS identified the transfers carried out by EUIs (or by private entities on their behalf) in the context of contractual relationships with organisations based in the US as deserving priority attention. In order to streamline compliance and enforcement measures, the strategy distinguishes between short-term and medium-term compliance actions.

EUIs were requested to carry out a mapping exercise and to report to the EDPS on certain types

of transfers. In 2021, the EDPS will provide guidance and pursue enforcement actions for transfers to the US or other non-EU countries on a case-by-case basis in line with the strategy.

### 3.2.2 The Hague Forum for Cloud Contracting & use of Microsoft products and services

The Hague Forum for Cloud Contracting, co-established by the EDPS, is a cooperation platform for public authorities, EUIs and other international and non-governmental organisations to ensure compliance with data protection law when using IT services, including cloud service and communications providers. The aim is to exchange information and take back control by strengthening negotiation power with service providers. The forum met for the second time on 2 July 2020.

On this occasion, the EDPS issued a [Public Paper](#) detailing its findings and recommendations of the EDPS investigation into the use of Microsoft products and services by EUIs. These findings aim to help public administrations to keep control and ensure an adequate level of data protection when contracting IT services. Based on the similarities between the GDPR and Regulation (EU) 2018/1725, applicable to EUIs, the findings of the EDPS investigation proved to be of interest to other public authorities as well. The Public Paper emphasises that when EUIs enter into contractual relationships with IT service providers, they should reinforce their control over how and why personal data is processed, as outlined in the EDPS’ strategic objective on ‘digital sovereignty’ from the [EDPS Strategy 2020-2024](#).

To this end, the EDPS issued a series of recommendations to ensure compliance with Regulation (EU) 2018/1725 and take back control over the processing of personal data. In particular, it is recommended to put in place compliant contractual terms to clarify the role and responsibilities of the data processor, control the use of subcontractors, data location, international transfers, and the risk of unlawful disclosure of data to mitigate risks for the rights and freedoms of individuals.

The European Data Protection Supervisor, Wojciech Wiewiórowski, pointed out that The Hague Forum is an example of the type of cooperation he wants for his mandate, with smart public authorities reinforcing the role of controllers and promoting responsible data processing in accordance with European values.

### 3.2.3 EDPS internal and external efforts on digital freedom

The EDPS is interested in policy initiatives to achieve ‘digital sovereignty’, where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with European values. At the same time, we are committed to overcome the detrimental vendor’s lock-in syndrome in EUIs.

Given the teleworking modalities in place for most of 2020, the EDPS, starting its own digital transformation process, began to explore free software alternatives to video conferencing and cloud collaboration software, that allow for on-premises installation, and carried out tests. The conference system Big Blue Button was used for a few public events.

Furthermore, the EDPS decided to evaluate two new social media channels for short messages and videos. The aim is to offer a privacy-friendly alternative to the established third-party social media channels. All these efforts will continue in 2021.

At the same time, the EDPS has been vocal in raising awareness about digital sovereignty to achieve data protection compliance in practice in a number of public events and among other EU institutions.

### 3.2.4 EDPS own-initiative Opinions

The EDPS has 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 the EDPS’ 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.

On 6 January 2020, the EDPS issued a [Preliminary Opinion](#) on the GDPR’s special regime which affords a degree of flexibility for scientific research carried out in the public interest and operating within an ethical framework. This regime applies the principles of lawfulness, purpose limitation, and protecting individuals’ data protection rights, but allows certain derogations from data controllers’ obligations. The EDPS acknowledges that the boundary between private sector research and traditional academic research is blurrier than ever. In its Opinion, the EDPS recommends intensifying discussions between DPAs and ethical review boards, to establish a common understanding of genuine research through the standardisation of EU codes of conduct, a closer alignment between EU research framework programmes and data protection standards. Debating when researchers’ access to data held by private companies can be provided for matters of public interest should also be addressed.

On 7 September 2020, the EDPS published a [blogpost](#) reflecting on the European Commission’s [Communication - A European strategy for data](#) and its [White Paper on Artificial Intelligence - A European approach to excellence and trust](#). The EDPS emphasises that any new regulatory framework for AI should be the same for both EU Member States and EUIs. The EDPS advises prudence, as AI should serve individuals and society as a whole and be subject to a proper benefits, costs and risks assessment of its impact upon them. The EDPS supports a moratorium on automated recognition in public spaces of human behavioural or biometric features and encourages the clarification of the scope and purposes that determine when it may be beneficial to nudge individuals to ‘volunteer’ their data to contribute to the greater good.

On 27 July 2020, the EDPS published an [Opinion](#) and a [Press Release](#) on the European Commission’s [action plan](#) for a comprehensive Union policy on preventing money laundering and terrorism financing (AML/CFT). In its Opinion, the EDPS encourages the Commission to make data protection a gold standard in this critical field. The EDPS underlines that governance mechanisms





should establish a clear legal basis for the processing of personal data, as well as rules for its access and sharing. The EDPS recommends safeguards in future legislation for data minimisation, purpose limitation and data protection-by-design, and the right to be informed. The EDPS supports Public-Private Partnerships (PPPs) between Financial Intelligence Units, law enforcement authorities and private sector for data-protection compliant research, but is concerned that PPPs for the sharing of operational information on intelligence suspects may carry an unacceptably high risk for individuals and their personal data. The EDPS also supports data protection principles in respect of international AML/CFT standards.

On 17 November 2020, the EDPS published a [Preliminary Opinion on the European Health Data Space \(EHDS\)](#), a platform for exchanging health data and fostering medical and scientific research. The EDPS supports the EHDS objectives, and stresses that protecting individuals' personal data should be a priority within its development. The EDPS advises the European Commission to clearly demarcate the nature, categories, and purpose of the data being processed, along with pinpointing the roles and responsibilities of each of the actors making this data available. Additionally, the technical requirements of the EHDS should ensure the right to data portability. The EDPS considers that solidarity between EU Member States, data protection authorities, EHDS users and healthcare professionals combined with an entrenched data governance mechanism embodying EU values will ensure the ethical, responsible and safe processing of personal data.

In all these contexts, the EDPS will continue to monitor the policy and legislative developments and their impact on data protection as part of the [EDPS 2020-2024 Strategy](#).

### 3.3 Supervising EUIs

As the data protection supervisory authority of the EU institutions and bodies, the EDPS is responsible for ensuring that the EU institutions respect the relevant data protection rules. The EDPS strongly believes that the EU institutions must lead by example, setting the standard for other organisations

and businesses in the EU to follow.

To fulfil this objective, the EDPS:

- responds to consultations from EUIs;
- addresses complaints about the EUIs; and
- produces papers and policies advising EUIs.

Article 58 of [Regulation \(EU\) 2018/1725](#) confers upon the EDPS a wide range of investigative powers for the performance of its tasks. The EDPS exercises these powers on a case-by-case basis and consistently aligns its approach with what is considered the most likely to produce positive results for individuals.

In cases where it is found that EUIs have not complied with the data protection rules, the EDPS can use corrective powers.

The EDPS also holds specific powers when supervising the [Area of Freedom, Security and Justice \(AFSJ\)](#).

The EDPS' role is to ensure the effective protection of individuals' fundamental rights and freedoms against the misuse of technologies, in particular in relation to EUIs' processing of personal data.

On 8 May 2020, the EDPS issued a [Public Paper](#) to explain how it will undertake one of its main tasks, under [Article 57](#) of Regulation (EU) 2018/1725, to monitor and enforce the application of the Regulation, detailing as well what is expected from EUIs.

The Public Paper emphasises that EUIs are responsible for complying with the Regulation and for demonstrating how they have complied with the said Regulation (accountability). The first line of defence is the responsibility of staff in the EUIs. The second line are the EUIs' own internal control mechanisms, in particular data protection by design and by default, organisational and technical safeguards, documentation of processing operations (including DPIAs), responding to individuals' inquiries and consulting their DPO. DPOs should

have appropriate resources and are the main contact point between EUIs and the EDPS.

As the data protection authority responsible for the processing of personal data by EUIs, the EDPS is a further line of defence and our main activities ([see Chapter 1: About the EDPS](#)) mirror those of national DPAs, albeit in a specific international public sector environment. Article 58 of the Regulation gives the EDPS a wide array of corrective and investigative powers, as well as powers to limit or ban processing operations and to impose administrative fines. We strive to be as transparent as possible in our work.

### 3.3.1 Consultations

EUIs can consult the EDPS for guidance on their planned processing operations and compliance with data protection law. Depending on the complexity of the EUI's request, the EDPS provides advice in different forms, via calls to the DPO hotline, informal advice to staff and formal signed letters, for example. However, whilst the EDPS provides guidance, the responsibility for ensuring compliance with data protection law remains with the EUIs.

Regulation (EU) 2018/1725 may also oblige EUIs to consult the EDPS on planned processing operations, particularly when they intend to adopt internal rules restricting individuals' right to data protection and with regard to extra-EU transfers of personal data that require prior authorisation. When replying to such requests, the EDPS provides input on any necessary improvements to be made.

On 8 May 2020, the EDPS issued a [Policy Paper](#) to provide guidance to EUIs and their DPOs on consulting the EDPS in the field of [Supervision and Enforcement](#). The Policy Paper situates consultations in the general accountability architecture of Regulation (EU) 2018/1725. The EDPS encourages EUIs to channel consultations through their DPO, who may resolve the issue internally and who is also the main interlocutor for the EDPS. The Policy Paper outlines when EUIs can or have to consult the EDPS, the analysis that the EDPS may undertake upon receipt, deadlines for the EDPS to reply, the format of the EDPS' reply and the scope for publication and follow-up by the EDPS.

In 2020, the EDPS issued 65 formal and informal Opinions, including consultations carried out in the supervision of the [AFSJ](#). EDPS Opinions cover a broad range of topics, from administrative measures, such as implementing rules on data protection and restrictions to individuals' right to data protection, to general questions relating to data protection issues such as COVID-19-related applications, consent, and the roles of data controllers and processors. The sections below provide a description of a selection of consultations issued in 2020; the list being therefore non-exhaustive.

#### Internal rules on restrictions to data subjects' rights

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

EUIs may restrict individuals' right to data protection on the basis of 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 the 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 2020, the EDPS issued 14 comments on draft internal rules on restrictions to individuals' right to data protection submitted by EUIs. Our most common recommendations to EUIs were in relation to the need to clarify or specify the scenarios in which restrictions take place, to make a clear link between processing operations in which restrictions may be imposed, and the relevant legal grounds. Our recommendations also include the requirement to conduct a necessity and proportionality test.

### The notion of “large scale” under Article 39(3)(b) of Regulation 2018/1725

The EDPS was [informally consulted](#) on whether a particular processing operation of individuals’ personal data was considered as a large-scale processing under [Article 39\(3\)\(b\)](#) of Regulation (EU) 2018/1725. Whilst the term large scale is not explicitly defined in EU data protection law, the EDPS notes that it is nevertheless an important concept which may require an EUI to carry out a DPIA. A DPIA ensures the identification and mitigation of any risks to the fundamental rights and freedoms of individuals.

The EDPS considered two factors to determine the meaning of large-scale processing, namely:

- the proportion of the relevant population, as per [Article 29](#) Data Protection Working Party’s Guidelines on DPOs which also refer to the number of individuals concerned; and
- the nature of the personal data processed and related risks, with reference to a non-exhaustive list of data processing operations that may represent a high risk enumerated within Article 35(3) and to corresponding information within Recital 91 of the GDPR.

### Payroll services for employees in non-EU countries

In April 2020, the EDPS [addressed](#) an EUI’s question about the data protection provisions to be included in an agreement with a service provider concerning payroll services for its local employees located in a country outside of the EU with which there is no adequacy decision.

The EDPS referred to the relevant provisions of Regulation (EU) 2018/1725, i.e. concerning grounds for transfers in [Chapter V](#), including derogations, should never lead to the possible breach of fundamental rights. The EUI’s personal data cannot be processed (solely) in accordance with guarantees provided by the law of the non-EU country.

The EUI, as a data controller, must ensure that the service provider, as a data processor, demonstrates

appropriate guarantees and safeguards for the processing.

### The APPF’s powers and data protection obligations

The Authority for European Political Parties and European Political Foundations (APPF) consulted the EDPS on the relationship between its powers and the data protection rules. The APPF conducts administrative investigations, which involves the processing of personal data for registering, monitoring and imposing sanctions on European political parties and foundations.

On 26 February 2020, the EDPS issued an [Opinion](#) to highlight that EUIs must observe high standards of data protection on the basis of Regulation (EU) 2018/1725. In its Opinion, the EDPS also highlights that the GDPR does not prevent third parties from disclosing personal data to EUIs with investigative powers when there is a legal obligation to do so, because there are lawful grounds for processing, and that EUIs may in some cases benefit from exemptions to notifying individuals concerned by the investigation.

### Consultations on personal data transfers by EUIs

The EDPS issued two Opinions relating to the legal basis for personal data transfers to an International Organisation (IO).

In the [first Opinion](#), an EUI wanted to use the meeting facilities of an IO for their meeting, which entailed the processing and transfer of participants’ names to the IO for security and organisational purposes.

In the [second Opinion](#), an EUI wanted to enable their staff to participate in training sessions organised by IOs, which similarly involved the processing of their personal data.

The EDPS highlighted that the parties should sign a legally binding and enforceable instrument, in accordance with [Article 48\(2\)\(a\)](#) of Regulation (EU) 2018/1725, to facilitate the processing of personal

data. However, should they be unable to do so, the most appropriate transfer tool is an administrative agreement, as outlined in Article 48(3)(b) of the Regulation.

The EDPS also provided analyses of the distribution of roles between EUIs and IOs and their legal consequences.

### Access to a complaint file at ERA

The [European Agency for Railways](#) (ERA) consulted the EDPS as to whether they could disclose a complaint based on the Staff Regulations to non-voting members of the ERA's Management Board (MB). The EDPS considered the disclosure lawful on the legal basis of the powers conferred to the MB, by the ERA's own Founding Regulation. However, the EDPS stressed that the disclosure should be without prejudice to rules on conflict of interest and noted the need for the ERA to review the personal data to be provided to members of the MB in light of the accountability principle.

The EDPS also highlighted the need to strike the right balance between data protection and transparency.

### 3.3.2 Surveys

In 2020, the EDPS launched two surveys.

The EDPS launched a survey in February 2020 to find out how EUIs have implemented DPIA tools so far, and published a [Report](#) in July 2020 on the positive outcomes of the survey as well as points for improvement. ([See section 3.3.6 on DPIAs.](#))

In December 2020, the EDPS launched a survey among EUIs aiming to investigate processing operations, IT tools and solutions implemented during the pandemic. ([See section 3.1.2 on Supporting EUIs as employers.](#))

### Complaints per institution

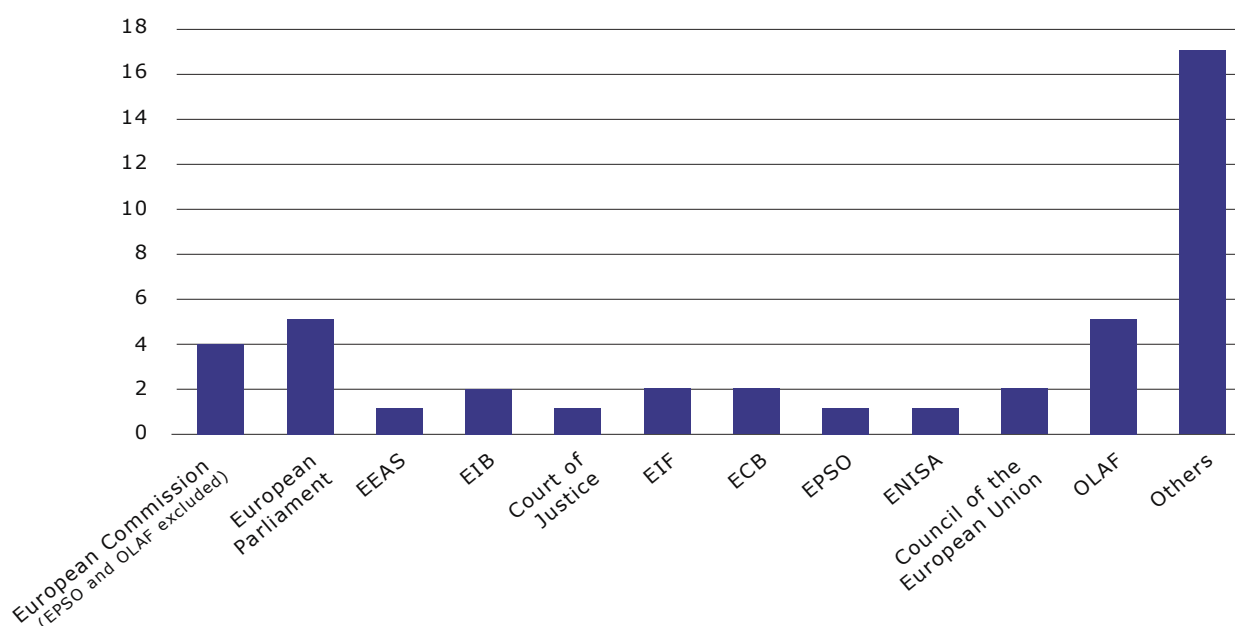


Figure 2. Complaints per institution



## Number of complaints received

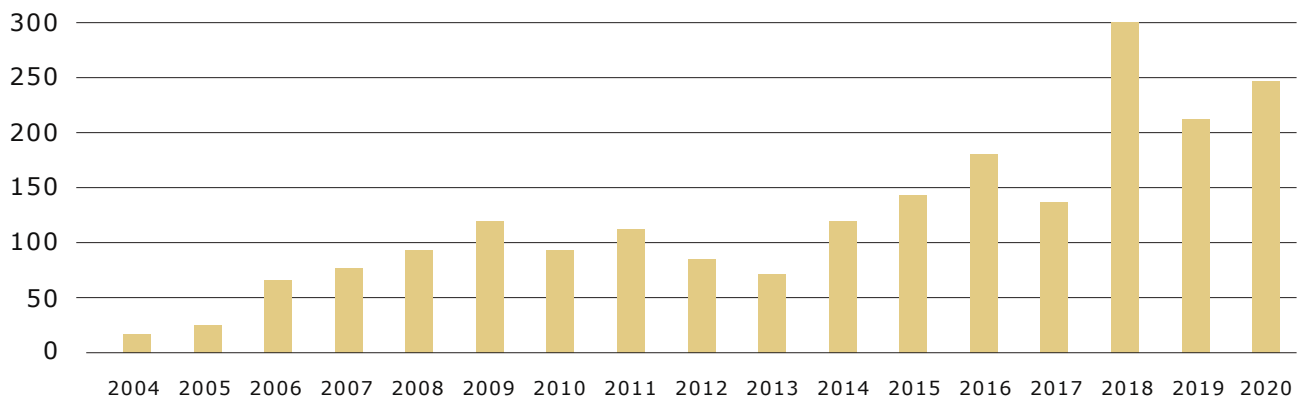


Figure 3. Evolution of the number of complaints, including inadmissible complaints, received by the EDPS

### 3.3.3 Complaints

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. Furthermore, staff members of the EUIs can submit complaints without being personally affected by the alleged infringement of the Regulation.

In 2020, the EDPS received 246 complaints, an increase of 16% compared to 2019. Of these, 203 were inadmissible, the majority relating to data processing done by national authorities or private entities as opposed to processing by an EUI. We replied to all inadmissible complaints, directing the complainant to the relevant authority. The remaining 43 complaints, representing a decrease of 28% compared to the previous year, required in-depth inquiry. In 2020, we issued 35 decisions on admissible complaints.

#### The right to access personal data in selection procedure

The EDPS issued a decision on a complaint against an EU institution concerning right of access in the context of a selection procedure. The complainant claimed that he had not been given access to their evaluation results in an intelligible form, since he had only been given a heavily redacted version, which only showed their scores and not the assessment criteria. The scores alone did not allow

the complainant to understand their results in the selection competition.

The EDPS found that the complainant should be given access to the specific assessment criteria, corresponding to the respective score obtained. Without them, the complainant would not be able to make sense of the results. The EU institution argued that disclosing the assessment criteria would jeopardise the objectivity and secrecy of future selection procedures since the same assessment criteria is likely to be used in other selection procedures. To eliminate this risk, the EDPS recommended that the EU institution invite the complainant to their premises for an on the spot access to a redacted version of the evaluation results, while presenting the information in an intelligible and transparent format.

In a complaint decision against another EU institution, the EDPS confirmed the candidates' right to access the assessment criteria and reasons for not being pre-selected in a recruitment procedure. The EU institution argued that since the selection procedure and the database where successful candidates were registered had been annulled following a judgment of the CJEU, no processing of the complainant's personal data had been carried out and the EUI in question no longer held any of their personal data. It further argued that passing tests or being registered in the database is not a guarantee of recruitment.

The EDPS found that the complainant's right of access is a continuous and permanent right, regardless of the fact that the selection procedure had been annulled. The EU institution had indeed processed the complainant's personal data when it initially assessed the complainant's application. The inquiry showed that the EU institution had applied objective criteria relating to language skills when deciding not to pre-select the complainant. For [accountability](#) purposes, the EU institution is required to keep a record of the documents and information on the complainant that had been processed during the pre-selection phase, including the reason for not pre-selecting them. The institution should apply a retention policy for each category of personal data, depending on the purpose for which they were processed and continue to be processed throughout the selection procedure and beyond.

Although EU institutions are not responsible for ensuring that all candidates in a selection database are recruited, they are accountable for ensuring that the data protection rules and principles are duly applied throughout the whole selection procedure, including the obligation to ensure that the candidates' right of access is respected.

### 3.3.4 EDPS Audits

As part of our supervisory work, we regularly conduct [audits](#) to verify how data protection is applied in practice by EUIs. We ensure that we cover EUIs of all sizes in our annual audit planning. The EDPS chooses to audit an EUI by taking into account a number of factors, including a risk analysis, whether special categories of data are processed, the time elapsed since the last audit or whether there has been an increase in the numbers of complaints.

During an audit, we typically meet the staff members responsible for processing data at the EUI and request information or demonstrations. During 2020 however, the EDPS carried out audits remotely due to the COVID-19 pandemic, so as to continue to provide assurance in respect of data protection compliance in the EUIs.

In early 2020, the EDPS conducted an audit to screen EUIs' compliance with [Article 31\(5\) of](#)

[Regulation 2018/1725](#), which states that: "Union institutions and bodies shall keep their records of processing activities in a central register. They shall make the register publicly available". We have previously issued guidance that making the register "publicly available" means publication on the internet. We conducted the first phase of the audit remotely and unannounced to determine whether the registers were available on the EUIs' websites, if these registers contained records as per the EDPS' (or comparable) template and the plausibility of the number of records listed. At the end of the second phase, we considered that only 15 out of a total of 67 EUIs examined were fully compliant.

Subsequently, we carried out another audit in respect of 27 EUIs' newsletters, focusing on the accessibility and transparency of the corresponding data protection statements, which aim to inform an individual on how their personal data will be processed when they subscribe to the newsletter.

### 3.3.5 EDPS Investigations

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

Our investigative powers allow us to:

- order controllers and processors to provide information required for our tasks;
- obtain access to all personal data and to any premises of the controller and the processor. This includes any data processing equipment and means of processing.

### EUIs and Microsoft products – findings

The EDPS completed an investigation into EUIs' use of Microsoft products and services. On 24 March, the EDPS issued its findings and recommendations to all EUIs; a [summary](#) of these findings was then published on 2 July 2020.



Our investigation focused on the risks posed by a corporate licensing framework agreement signed with Microsoft in 2018 to which all EULs could adhere to procure its products and services. We made the following key findings, accompanied by a set of recommendations to follow in renegotiating the arrangement with Microsoft.

First, the agreement allowed Microsoft to define and change the parameters of its processing activities carried out on behalf of EU institutions and contractual data protection obligations. The discretion that Microsoft had amounted to a broad right for Microsoft to act as a controller. Given the EU institutions' role as public service institutions, the EDPS did not consider this appropriate. The EDPS recommends to EU institutions that they act to retain controllership.

Second, EU institutions need to put in place a comprehensive and compliant controller-processor agreement and documented instructions of the EU institutions to the processors. Their lack of control over which sub-processors Microsoft used and lack of meaningful audit rights also presented significant issues. The EDPS makes recommendations on how to improve the controller-processor agreement and put robust audit checks in place.

Third, EU institutions faced a number of linked issues concerning data location, international transfers and the risk of unlawful disclosure of data. They were unable to control the location of a large portion of the data processed by Microsoft, nor did they properly control what was transferred out of the EU/EEA and how. There was also a lack of proper safeguards to protect data that left the EU/EEA.

EU institutions also had few guarantees at their disposal to defend their privileges and immunities, and ensure that Microsoft would only disclose personal data insofar as permitted by EU law. The EDPS made recommendations to assist EU institutions in addressing these issues.

Fourth, the EDPS considered the technical measures that the Commission had put in place to stem the flow of personal data generated by Microsoft products and services and then sent to

Microsoft. As such, the EDPS recommends that all EU institutions perform tests using a revised and comprehensive approach, share among them the knowledge and technical solutions they developed to prevent unauthorised data flows to Microsoft and inform each other of any data protection issues they identify with the products or services.

Fifth, the EU institutions had insufficient clarity as to the nature, scope and purposes of the processing and the risks for individuals' personal data to be able to meet their transparency obligations towards them. The EDPS recommends that EU institutions seek the clarity and assurances allowing them to keep individuals properly informed.

### **EDPS investigation on the European Parliament's WIFI**

Activities taking place in the context of (the European Parliament's) Wi-Fi networks must comply with the requirements of Regulation (EU) 2018/1725, insofar as they concern processing of personal data. The EDPS found a significant issue regarding the definition of personal data processing, which consequently had an impact on the transparency of the processing and the information to be provided to individuals. The EDPS further identified additional issues, mainly technical, for example the technical and organisational measures relating to the security of processing as well as the security and confidentiality of transmissions and transfers of personal data in the context of investigations.

In summary, the EDPS found that IP addresses, recorded when using the European Parliament's Wi-Fi network services, are not recorded in isolation. In combination with other attributes (such as the MAC address, which can uniquely identify a device, the connection time and the access point to which the device is connected), there is the possibility for individuals to be identified, either by the data controller or by another entity that may obtain access to this information.

The EDPS issued an order under [Article 58\(2\)](#) of Regulation (EU) 2018/1725, requesting immediate action to remedy the identified infringement, as well as a number of recommendations aiming at the overall improvement of the processing operations

within the scope of the [investigation](#).

The investigation was carried out in 2020; a final decision based on its findings was issued in 2021.

### Cooperation with the EFTA Surveillance Authority

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

In 2020, the EDPS continued its advisory work with ESA. Over the last year, following the adoption of [Decision 100/19/COL](#) (laying down a set of rules closely aligned with Regulation (EU) 2018/1725), the ESA has been transitioning not only to an updated data protection regime but also to a new location. The EDPS assisted ESA, by providing guidance on data protection questions affecting its daily operation.

### 3.3.6 Advising and Guiding EUIs

One of the key roles of the EDPS is to supervise the compliance of EUIs with Regulation (EU) 2018/1725. One of the ways the EDPS ensures that EUIs are consistently complying with data protection law is by advising, guiding and collaborating with their [DPO](#). The DPO plays an important role as interlocutor and key contact point between the EDPS and their EUI.

#### Adapting our Guidelines

A key approach through which the EDPS provides guidance is by updating and adapting guidelines to give the appropriate tools for DPOs and data controllers to ensure compliance with Regulation (EU) 2018/1725.

#### Updating Guidance on Article 25 of Regulation (EU) 2018/1725

Data protection is a fundamental right which contains ‘rights within the right’ such as the rights

of information and access, among others. Whilst these rights are to be strictly respected and ensured by EUIs, the previous Regulation 45/2001 provided for restrictions which could be adopted on a case-by-case basis. However, under Regulation (EU) 2018/1725, restrictions must also be backed by a secondary EU legal act, or be based on matters relating to the operations of an EUI backed up by fully-fledged internal rules adopted at its highest level. Since it is mandatory for EUIs to consult the EDPS when drawing up such internal rules, the EDPS receives dozens of consultations on the topic since the entry into force of Regulation (EU) 2018/1725 in December 2018. The EDPS therefore updated its [Guidance](#) to reflect the new development.

In the Guidance, the EDPS reminds what constitutes a restriction of individuals’ right to data protection, noting that while such rights may be restricted, they cannot be denied and restrictions must be temporary in nature. The EDPS notes specifically which rights may be restricted, as well as the conditions for any restriction, including the necessity and proportionality test and the need to establish a legal basis. The EDPS provides practical advice on how to draft internal rules and how to implement them, noting the need for such rules to be clear and precise.

#### Revised eCommunication guidelines

In February 2020, the EDPS issued [Guidelines on electronic communications](#) (eCommunications), which encompasses the use of emails, telephony and internet in the daily operations of EUIs. The Guidelines update the earlier text issued in December 2015 and reflect the new rules introduced under Regulation (EU) 2018/1725. Since eCommunications include the processing of EUI staff members’ personal data, the EDPS provides recommendations to ensure compliance with data protection law in this context.

The Guidelines include recommendations for processing personal data in the framework of system security and traffic management, in which internet monitoring must be limited to those purposes, as well as billing and budget management. The EDPS notes the requirement to process only the necessary personal data to achieve a specific purpose, and to

ensure staff are informed of the EU's personal data processing policy. In addition, the EDPS provides a reminder of the key principles of data protection, which are to be complied with in the context of eCommunications, including the right to access and rectification, keeping personal data accurate and up-to-date, and keeping personal data secure.

### Data Protection Impact Assessments (DPIAs)

The DPIA is an important tool of data protection law through which organisations assess and mitigate risks for the rights and freedoms of individuals that may arise when processing sensitive data. In February 2020, the EDPS conducted a survey to determine specifically how EUs have been using DPIAs since the entry into force of Regulation (EU) 2018/1725.

In July 2020, the EDPS published a [Report](#) based on a survey carried out in February 2020 on how EUs carry out DPIAs. The Report contains lessons learned and best practices observed by the EUs. The aim of the Report is not only to highlight good practice, but also to provide additional supporting guidance to EUs as they carry out DPIAs. In the Report, the EDPS outlines how EUs may decide whether or not to carry out a DPIA and provides examples of the threshold assessments already conducted in this context. The Report also notes the involvement of the DPO in the different stages of the DPIA process and highlights some of the lessons learned in the process of doing a DPIA. For example, it is recognised that data protection needs are to be flagged early on and require sustained focus over time. Special caution is required regarding the involvement of data processors or third parties as well.

In addition to the Report on DPIAs, the EDPS published a 'DPIA in a nutshell' [Factsheet](#) as an easy-to-access one page guide for DPOs. Due to the central role that DPOs play in the process of carrying out a DPIA, the EDPS also released a [video](#) on the subject to act as a friendly and accessible tool for DPOs.

### Flowcharts, quick-guides and checklists on data protection

In 2020, the EDPS published user-friendly [Flowcharts and Checklists](#) with the aim of making data protection more accessible to DPOs and their EUs. By presenting key data protection principles and data controller and processor tasks in step-by-step flowcharts, the EDPS facilitates compliance with the requirements set out in Regulation (EU) 2018/1725. In the flowcharts and checklists, the EDPS outlines the duties of data processors and data controllers, what is required in a data processing agreement, and notes the implications of Brexit on data transfers. In addition, the EDPS outlines its powers under Regulation (EU) 2018/1725 and the administrative fines and sanctions.

In January 2020, we also published [the EDPS quick-guide to necessity and proportionality](#). The processing of personal data constitutes a limitation of the right to the protection of personal data and therefore must comply with EU law by ensuring that the measure is both necessary and proportional. The guide outlines 8 steps to help EUs and their DPOs to assess the compatibility of measures impacting the fundamental rights to privacy and protection of personal data with the EU Charter of Fundamental Rights.

### A tailored approach to workshops and training sessions

Throughout 2020, the EDPS organised numerous training sessions for EUs on themes that we identified as areas in which further clarity or assistance to ensure compliance with Regulation (EU) 2018/1725 is required. For example, the EDPS organised training sessions on the relationship between data controller and processor and joint controllership, data protection in procurement and on outsourcing the processing of personal data, and on international data transfers.

In addition, the EDPS also organised on-demand training sessions requested by EUs and their DPOs, focusing on data protection operations and their implications in relation to the EU's core activities and area of business. The on-demand sessions include expert presentations on the subject, case



studies, and practical examples that DPOs may encounter.

### Overview of training sessions

It is custom for the EDPS to organise multiple training sessions per year; 2020 was no exception, although most training sessions were held remotely due to COVID-19. Training sessions are either organised following the request of the data protection officer (DPO) or data protection coordinator of an EUI, or at the EDPS' own-initiative to raise awareness about a particular data protection issue.

Throughout the year, the EDPS organised training sessions on a number of pertinent subjects, such as the application of data protection rules in different contexts, for example in event management, procurement procedures. Other [training sessions](#) focused more on the rights of individuals and the obligations of controllers, processors and DPOs under Regulation (EU) 2018/1725. Transfers of personal data to non-EU countries were also high on the agenda.

Within the EDPS, training sessions are also organised in collaboration with other units. For example, in October 2020, the Supervision and Enforcement Unit (S&E) and the Technology and Privacy Unit (T&P) delivered training sessions to the [European Intellectual Property Office](#) (EUIPO). S&E's training session focused on the application of data protection principles in the context of remote working, among other topics; while T&P exchanged views with EUIPO on data protection challenges of digital transformation, including the use of artificial intelligence, blockchain and other cutting-edge technologies.

Training sessions are a way for the EDPS to both support and ensure that EUIs comply with EU data protection laws. To ensure an interactive training session with learning outcomes that EUIs can easily put into practice, the EDPS always organises training sessions with case studies directly related to a particular EUI's core business activity.

### EDPS meetings with the network of DPOs of the EUIs

Due to the important role played by DPOs as interlocutors 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 for the DPOs of EUIs and to identify areas where extra guidance or support from the EDPS is needed.

In light of the COVID-19 pandemic, the EDPS organised the [47th meeting of the network of DPOs](#) virtually on 8 May 2020. This marked the first remote DPO meeting using videoconference facilities, which was nevertheless a lively and dynamic discussion with 117 participants. The issues covered included the use of social media as a means of communication for EUIs, both to inform the public and acting as a source of information. The meeting also covered the EDPS' investigation into the use of Microsoft services by EUIs. Importantly, challenges faced by DPOs were also discussed, the processing of personal data in the context of COVID-19, as well as the best practices relating to the publishing of data protection registers.

On 11 December 2020, the [48th meeting of the network of DPOs](#) was held remotely. The second meeting was an opportunity for DPOs to express their concerns related to international transfers in light of the "[Schrems II](#)" ruling and the EDPS' recently published [Compliance Strategy](#). Since the EDPS is fully aware of the fact that the implementation of the "Schrems II" Judgment presents serious challenges for EUIs, the meeting was particularly pertinent for providing guidance. Questions from DPOs focused on technical details linked to complying with the Judgment, particularly in relation to the practical consequences for new and existing contracts, how to conduct Transfer Impact Assessments (TIAs), and the margin of manoeuvre regarding the alternative transfer tools and the importance of supplementary measures.

The second part of the meeting, called "Technology, Privacy in 2020 and beyond – a futuristic retrospective" provided DPOs with an update of the tech challenges in protecting personal data and privacy. There was also time to reflect on what 2021 may bring in this area.

## Website Evidence Collector

The Technology and Privacy Unit (T&P) originally launched the EDPS [Website Evidence Collector](#) (WEC) in 2019 as an open source software tool for DPAs, data controllers, data protection practitioners and web developers, to help them ensure that their websites are compliant with the General Data Protection Regulation (GDPR) and Regulation (EU) 2018/1725. In particular, the WEC helps them to better understand what information is stored during a visit to their websites, for example when browsing pages one after another without further user action, login or expressing consent. The EDPS received the Global Privacy and Data Protection Award for innovation in respect of the WEC at the 2019 [Global Privacy Assembly](#).

The EDPS will make the version 1.0 of the WEC available in 2021.

## 3.4 Supervising Area of Freedom, Security and Justice

In accordance with Title V of the [Treaty on the Functioning of the European Union](#), the Area of Freedom, Security and Justice (AFSJ) covers policy areas that range from the management of the European Union's external borders to the judicial cooperation in civil and criminal matters. It includes asylum and immigration policies, police cooperation and the fight against crime (terrorism, organised crime, trafficking in human beings, drugs, etc.).

As the data protection authority of Europol, Eurojust, EPPO, Frontex, EASO (European Asylum Support Office) or eu-LISA (European Union Agency for the Operational Management of Large-Scale IT Systems in the AFSJ), the EDPS is uniquely positioned to monitor data processing operations in this area. Among others, the EDPS monitors the development and adoption of new technologies, promoting solutions that protect individuals' rights and freedoms.

### 3.4.1 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 personal data processing by Europol, pursuant to [Article 43](#) of Regulation (EU) 2016/794 (Europol Regulation). In 2020, the extraordinary circumstances of COVID-19 forced the EDPS to postpone for the first time the annual inspection to Europol, which normally takes place in May or June every year. Nonetheless, the new reality encouraged the EDPS to engage even more closely with Europol during this term: regular contact at management level continued remotely, bi-monthly meetings with Europol's data protection team and staff members were held online every two to three weeks.

#### Supervision in the field of Big Data and Artificial Intelligence

In this term, the EDPS prioritised the monitoring of new technologies used by Europol, such as those involving [data analytics and artificial intelligence](#) with particular focus on two key areas.

First, the EDPS launched in April 2019 an inquiry into the processing of large datasets by Europol. The EDPS acknowledges that Europol's processing of such large datasets, collected by national law enforcement authorities in the context of criminal investigations, has become an important part of the work performed by Europol to produce criminal intelligence. However, while the processing of such information might be lawful under national law, the Europol Regulation is much more restrictive. In particular, Europol can only process information about certain categories of individuals, namely suspects, contacts and associates, victims, witnesses or informants and certain categories of data. The volume of information is so considerable that its content is often unknown until the moment when analysts extract the relevant entities for entry into the relevant database. Europol was not able to provide appropriate reassurance that all the personal data contained in its large datasets comply with the limitations set up by the Europol Regulation. As a result, the EDPS has decided to admonish Europol,

urging Europol to submit an Action Plan and to inform the EDPS about the measures put in place to address these concerns. Admonishments are meant to signal data processing activities that are not in line with the applicable data protection framework and to invite the agency to adjust its practices.

Second, Europol's plans to develop policies for the use of operational data for data science purposes, including the testing, development and training of algorithms has resulted in the launch of an EDPS inquiry. As such, the EDPS aims to get a clear understanding of the lawfulness of data processing activities taking place in this context and of the safeguards put in place to address the data protection risks linked to the use of machine learning tools.

### Cooperation regarding Brexit

On 17 November 2020, the EDPS issued an Opinion on procedures for handling UK data subject access requests following the Brexit transition period, clarifying that, from January 2021, individuals from the UK requesting access to their data should be considered alongside requests from other non-EU countries. Individuals from the UK will submit requests to one of the 27 competent authorities in a more restrictive procedure compared to the pre-Brexit one. The EDPS recommended that relevant parties inform individuals about the upcoming changes and advised that future arrangements providing cooperation between the UK and Europol should address this issue. The EDPS also pointed to the unharmonious situation in which Third Country Nationals (TCN) are when filing a request for access as they cannot submit their requests to Europol directly but should go through one of the appointed authorities in the EU Member States.

On 18 December 2020, the EDPS provided its agreement on the draft Decision of the Europol Management Board authorising a set of data transfers to the UK in accordance with [Article 25\(6\)](#) of Europol Regulation. The Decision would have provided a legal basis for cooperation between the UK and Europol in the absence of an agreement and in the absence of an adequacy decision legitimising data transfers. By relying on the derogation under Article 25(6) of the Europol Regulation and in

agreement with the EDPS, Europol would have been able to transfer personal data to the UK in light of adequate safeguards addressing the protection of privacy and fundamental rights and freedoms of individuals.

### Consultation on the deadline for data subject access requests during the COVID-19 crisis

Shortly following the outbreak of COVID-19, Europol sought the EDPS' advice on how to manage delays in responding to individuals requesting access to their data, as a result of the crisis. The EDPS advised that in case of delayed response, Europol must document reasons for such delays and develop a clear, proactive communication strategy. These contingency measures were intended to limit the adverse effects of delayed responses and ensure that individuals maintained an open communication channel with Europol. Ultimately, there was no need to invoke these measures, as Europol answered all requests within the legal timeframe.

### Consultations in the field of interoperability

In 2020, the EDPS continued ongoing discussions with Europol on the topic of interoperability, i.e. the ability for information systems in the area of security, border and migration management to facilitate information sharing through technical processes, standards and tools.

First, the EDPS received an informal consultation from Europol regarding their procedure to request Passenger Name Record (PNR) information from specialised units in EU Member States and on potential communication channels between Passengers Information Units (PIUs). Following on from last year's Prior Consultation on PNR data handling at Europol and the inspection of AP Travellers during the 2019 Annual Inspection, the EDPS will continue to pay specific attention to the processing of personal data in the field of travel information, which has been an increasing focal point for both Europol and the EU as a whole.







Figure 4. *Europol Statistics in 2020*

Second, the EDPS delivered an Opinion on the implementation of the new [Schengen Information System \(SIS II\)](#) legal framework at Europol. Adopted in December 2018, the framework aims to further enhance the system's capabilities, providing Europol with access to additional categories of alerts, including those on missing persons or people who are sought to assist with a judicial procedure. The EDPS stressed the importance of a structured internal framework for the processing of the SIS II data at Europol, capable of compensating for the removal of the previous legal limitations that existed in terms of accessible categories of SIS alerts.

Third, Europol submitted a prior consultation under Article 39 on the access to VIS. According to the [VIS Council Decision](#), Europol should be granted access to VIS in the course of its duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats. The establishment of the Visa Information System (VIS) represents one of the key initiatives within the policies of the European Union aimed at establishing an area of freedom, security and justice. VIS has the purpose of improving the implementation of the common visa policy and contributes towards guaranteeing internal security and combating terrorism under clearly defined and monitored circumstances.

### Other consultations

Another consultation concerned the Prior Notification of Online Service Provider Referral Systems. In recent years, flows of personal data in the field of child sexual exploitation material (CSEM) have increased exponentially, notably due to the efforts of the US National Centre for Missing and Exploited Children (NCMEC). The EDPS provided feedback on a proposed operational framework that would involve more closely EU Member States' investigators in determining national priority criteria and the ranking of referrals according to operational usefulness.

### 3.4.2 Supervising Eurojust

On 12 December 2019, a new supervisory framework for the processing of personal data at the EU Agency for Criminal Justice Cooperation ([Eurojust](#)) 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.

Fully promoting Eurojust's role in the coordination of EU Member States' judicial authorities investigating serious organised crime, the EDPS is determined to exercise its supervisory role and to enforce existing safeguards.

### Operational visits and regular meetings with Eurojust staff members and the data protection officer

Audits and visits are tools used by the EDPS to monitor EUJs and raise awareness about data protection. While audits are used to assess how well an EU institution is implementing data protection rules, visits are used to create a collaborative roadmap for the implementation of these rules.

In 2020, the EDPS held multiple meetings with Eurojust to ensure compliance with the latest data protection regulations. The EDPS worked closely with Eurojust's DPO and other operational staff in regular meetings, providing them with informal advice when needed. Due to the pandemic, six meetings were held remotely between the EDPS and the DPO of Eurojust.

In January 2020, the EDPS conducted an operational visit at Eurojust's premises and provided an induction awareness training to Eurojust staff on the supervision activities of the EDPS, focusing on data protection risks and personal data breaches.

Two visits to Eurojust were organised in February 2020. On 11 February 2020, the Supervisor was invited to participate in a meeting with the College of Eurojust during which he gave a speech addressed to the National Members of Eurojust.

On 16-17 February 2020, EDPS staff conducted an operational visit to Eurojust, focusing on the architecture and functioning of the Case Management System, as well as on its practical use by National Members of Eurojust. The EDPS used the visit to better understand Eurojust's practices and procedures through on-the-spot demonstrations of the Case Management System. The insights gained from this visit served for the preparation of an inspection scheduled for autumn 2020. Unfortunately, due to COVID-19 restrictions, this had to be postponed.

### Eurojust Consultations

In 2020, Eurojust has sought the EDPS' advice several times on how to best comply with the EU data protection regime.

As a consequence of the new EU data protection regime, Eurojust adopted [implementing rules \(IRs\)](#) on the DPO. The EDPS recommended Eurojust to clarify some IRs provisions, specifying responsibilities attached to its DPO. For the same reason, [new rules concerning restrictions under Article 25](#) of Regulation (EU) 2018/1725 were developed by Eurojust in consultation with the EDPS. Since the document is based on existing EDPS guidelines, only a few minor recommendations were issued.

Furthermore, a [consultation](#) was held regarding the legal basis for information exchange between Eurojust and the European Border and Coast Guard Agency (or [Frontex](#)). In this case, the EDPS emphasised that Eurojust can only transfer operational data to Frontex if the transfer is:

- necessary for the performance of Eurojust tasks;
- within the limited law enforcement competence of Frontex;
- in compliance with all other conditions included in national and European legal provisions;
- proportionate to the envisaged purpose.

### 3.4.3 Supervising the European Public Prosecution Office

The European Public Prosecutor's Office ([EPPO](#)) is the EU's first independent prosecution office, with the power to investigate, prosecute and bring to judgement large-scale, cross-border crimes against the EU budget, such as fraud and corruption. The EDPS has started preparations to supervise EPPO's activities since the EPPO Regulation came into force on 20 November 2017. At the request of EPPO and in the initial absence of a DPO, the EDPS seconded one of its staff member in order to facilitate EPPO's preparations in relation to its data protection obligations. From December 2019 to the end of

March 2020, the seconded expert provided practical advice to EPPO on various topics, including CMS development, data protection implementing rules and the DPO vacancy notice.

The first official meeting between the first Chief European Prosecutor Laura Codruța Kövesi and the European Data Protection Supervisor Wojciech Wiewiórowski took place remotely on 22 September 2020.

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

To ensure that the EDPS is best prepared to conduct its supervisory role, an external study is being carried out. The purpose of the study, which started in June 2020, is to analyse EPPO's legal framework to distinguish the supervisory role of the EDPS from the supervisory role of national DPAs and to identify any potential problems this may pose.

In 2020, the EDPS has continued to contribute to EPPO's development by providing recommendations on EPPO's [rules of procedure](#) and on EPPO's [rules on the processing of personal data](#). Consultations on [DPO rules](#) and [Article 25 restrictions](#) also took place.

Following the performance of a Data Processing Impact Assessment ([DPIA](#)) carried out for the EPPO Case Management System (CMS), the EDPS was [consulted](#) on the risks identified by the DPIA. The Supervisor underlined the overall good quality of the DPIA with regard to its content and the methodology used. Nonetheless, some points for improvement were identified, such as the need for a clearer delineation between 'events' and 'risks' and for a more concrete description of the mitigating measures. The EDPS also highlighted that some

risks should be further clarified and identified additional risks to consider.

### 3.4.4 Coordinating the supervision of large-scale information system

There are a number of [large-scale IT systems](#) that are currently active in the EU, including Eurodac, the Visa Information System (VIS), the Schengen Information System (SIS) and the Custom Information System (CIS).

The EDPS cooperates with national DPAs through the Supervision Coordination Group (SCGs) to ensure coordinated end-to-end supervision of all databases. Due to the pandemic, in 2020 the SCGs for Eurodac, the SIS, and the VIS met remotely in June and November. The SCG for the CIS met once remotely in June. The results of these meetings are published on their [respective webpages](#) on the EDPS website.

### Technical rules for the Schengen Information System

On 26 August 2020, the EDPS issued [Formal Comments](#) on the European Commission's draft Implementing Decisions on the technical rules regarding entering, updating, deleting and searching data in SIS II and on minimum data quality and technical standards for biometric data. The EDPS highlighted that processing personal data – especially biometric data – of a large number of people can have a significant impact on individuals.

The EDPS emphasised that it is essential that both the legal framework and technical rules applicable to SIS II are compliant with EU data protection law and highlighted that powers delegated to [eu-LISA](#), the agency responsible for the operational management of SIS II and other large-scale IT systems, should be rooted in a strong legal basis. Finally, the EDPS noted that the sub-delegation of the Commission's powers to a Union agency raises a number of questions related to legal competence, which must be closely monitored.

### The future of coordinated supervision

The data protection rules for the EU institutions and bodies, set out in Regulation (EU) 2018/1725, provide for a single model of coordinated supervision for EU large-scale IT systems and agencies within the framework of the EDPB. This will replace the current system of individual SCGs.

The new model will not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency becomes applicable.

Since 2018, preparatory work has been ongoing within the EDPB to organise this model, currently only applicable to the Internal Market Information system (IMI) and Eurojust. The EDPS has played an active part in this process.

To put the new model of coordinated supervision - envisaged by the legislator - into practice, the EDPB changed its rules of procedure in November 2019, in order to establish a [Coordinated Supervision Committee](#) (CSC). The CSC held its first meeting on 3 December 2019, during which its own Rules of Procedure were adopted and a coordinator was appointed. Two meetings of the CSC have taken place, in July 2020 (during which its Work Programme 2020-2022 was adopted) and December 2020.

## 3.5 Technology and Privacy

Data protection has a strong connection with technology. The integration of computers within the business and public administration domains triggered the development of data protection laws and principles, which in turn led to the creation of data protection authorities (DPAs).

DPAs must keep abreast of both the potential risks and opportunities offered by technological advances. They invest to understand the possibilities of new technology and at the same time encourage the integration of data protection by design and data protection by default into the innovation process.

The EDPS places strategic importance on integrating the technological dimension of data protection into our work. This work is undertaken by our specific unit created in 2019 and renamed in 2020 as the Technology and Privacy Unit (T&P).

T&P monitors, advises and acts upon technological developments and trends via our:

- blogposts and TechDispatch publication;
- organisation of events, training and workshops for EUIs and international organisations;
- promotion of privacy engineering, for example our organisation of the Internet Privacy Engineering Network ([IPEN](#)) workshops;
- establishment of the 'state of the art' in data protection by design, for example our contribution to the International Committee of the Red Cross (ICRC) [Handbook](#) on data protection in humanitarian action (Second edition) and The International Working Group on Data Protection in Technology ([IWGDPT / The Berlin Group](#));
- provision of the technological knowledge and tools to perform effective inspections of IT systems, and other technical solutions used as means to process personal data;
- remote and/or targeted audits, for example our [EUI Microsoft Investigation](#), EURODAC inspection report, Europol supervision, Frontex investigation, mobile app audit and our supervision of large-scale information systems; and
- management of personal data breach notifications from the EUIs.

### 3.5.1 TechDispatch

The EDPS regularly publishes [TechDispatch](#) reports to explain emerging developments in technology. Each TechDispatch provides factual descriptions of a new technology, assesses the possible impact on privacy and the protection of personal data, and provides links to further recommended reading.

We published three issues of TechDispatch in 2020. These addressed the privacy implications of:

- [contact tracing with mobile applications](#) to alert individuals who have been in contact with COVID-19 infected individuals. As both traditional and digital proximity contact tracing involve the processing of personal health data, special protection is needed. Data protection by design measures put in place to achieve data minimisation and privacy-enhancing technologies can prevent harm through identification of contacts and infected cases.
- [quantum computing](#) that can compromise data security and confidentiality of communications, as quantum computers have a speed advantage over classical computers for selected problems and could therefore perform types of computation not available to current classical computers. As a consequence, quantum computing has the ability to break cryptography and as such harm severely IT security, e.g. affecting internet protocols like HTTPS (TLS) used for secure browsing.
- the potential for [Personal Information Management Systems \(PIMS\)](#) to enable individuals to manage their personal data in secure local or online storage systems, to share this data when and with whom they choose and to keep track of who has had access to their digital behaviour.

### 3.5.2 Managing personal data breaches

Under [Article 34](#) of the Regulation (EU) 2018/1725, all EU institutions, offices, bodies and agencies (EUIs) have a duty to report personal data breaches to the EDPS, unless the risk for individuals is unlikely. Every EUI must do this immediately, and at the latest 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 must also inform the concerned individuals without unnecessary delay. Similar obligations apply to Europol under [Regulation \(EU\) 2016/794](#).

Risk assessment is a core element in preventing and responding to personal data breaches. Unlike other traditional risk assessment methodologies, the focus in a personal data breach is on evaluating the risk(s) for the rights and freedoms of individuals. While various stakeholders, data protection authorities (DPAs), private and public organisations use a range of different methodologies to do this, our [Guidelines on Personal Data Breach Notification](#) aim to simplify the task by providing guidance and practical examples to assist EUIs in their efforts. In 2020, we contributed to the [EDPB Guidelines 01/2021](#) on examples regarding Data Breach Notification by providing input on both the selection of scenarios and their assessment. We also delivered online training sessions to the European Union Intellectual Property Office (EUIPO) in the context of providing practical information to EUIs on assessing and notifying personal data breaches.

In 2020, the EDPS received and assessed 121 new personal data breach notifications under Regulation (EU) 2018/1725. Overall, there is an approximate 20% increase in the number of personal data breach notifications the EDPS received in 2020 compared to 2019.

A personal data breach occurs when there is either a breach of confidentiality, integrity or availability. In 2020, 93% of personal data breaches notified to us concerned a breach of confidentiality. While human error remains the most common root cause of the personal data breaches notified to the EDPS in 2020, an increase in the number of notifications received where the root cause was an external attack is also evident. Furthermore, the number of technical errors that caused personal data breaches doubled in 2020 compared to 2019.

Concerning the impact of the reported personal data breaches, more than half of these breaches affected 1-10 individuals, while around 24% of them affected 11-50 or 101-500 individuals. Only 8 out of the 121 data breaches affected more than 1000 individuals. Also, 23% of the total reported breaches affected special categories of data, such as health data and operational data (from activities by criminal justice authorities and police, falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU).



According to [Article 35](#) of Regulation (EU) 2018/1725, if the breach is likely to pose a high risk of adversely affecting individuals' rights and freedoms, the EUI must also inform the individuals concerned without undue delay. In 2020, data controllers decided to communicate the personal data breach to the affected individuals in 45 cases. While some were obliged to do so due to the high risks identified for individuals, others decided to notify the individuals as a matter of transparency.

The COVID-19 pandemic had an impact on personal data breaches among EUIs. The EDPS has received a few cases of security incidents mainly due to human error as a result of teleworking, because of the inability for EUI staff to access established tools automating processes, only accessible on site, and the need to deviate from standard procedures.

This also included human errors during recruitment processes as EUIs were forced to conduct these online.

In a few cases, personal data breaches also occurred in the context of manual contact tracing, where the identity of an individual diagnosed with COVID-19 was accidentally revealed to their close contacts, or the identity of a close contact of an individual diagnosed with COVID-19 was revealed to other contacts of the infected individual.

Due to the sensitivity of the personal data involved in these personal data breaches, and based on these concrete examples, the EDPS' Technology and Privacy Unit contributed to the EDPS' [Orientations on manual contact tracing by EUIs in the context of the COVID-19 crisis](#).

### Data breach notification per month in 2020

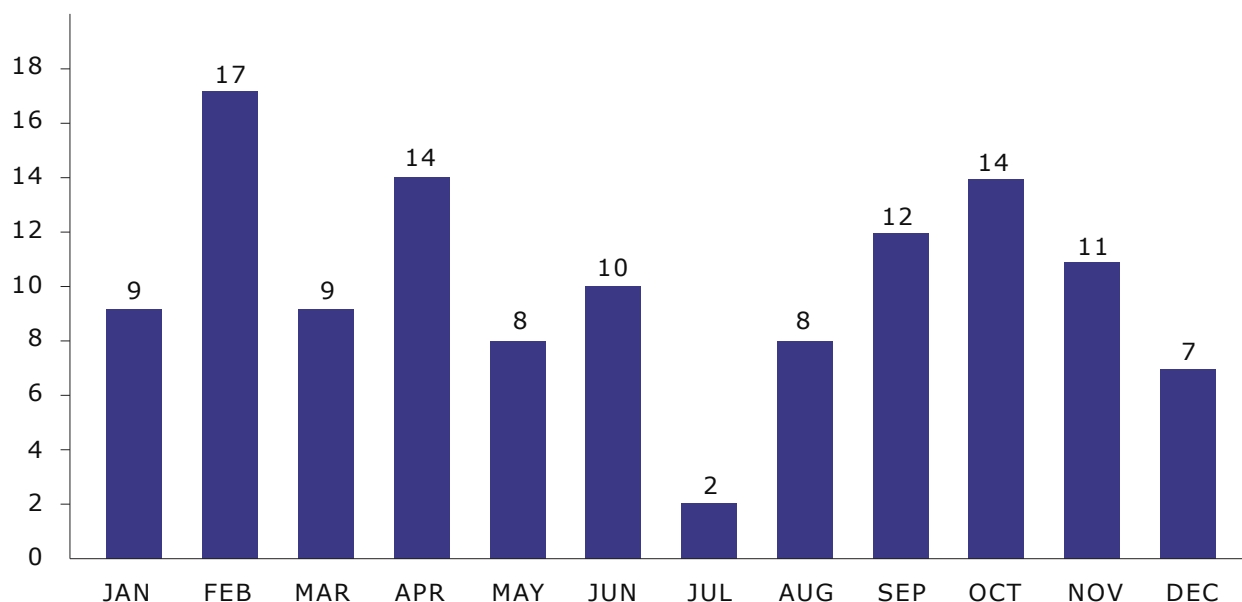


Figure 5. EDPS - Number of personal data breach notifications per month



### Personal data breach notifications 2019-2020

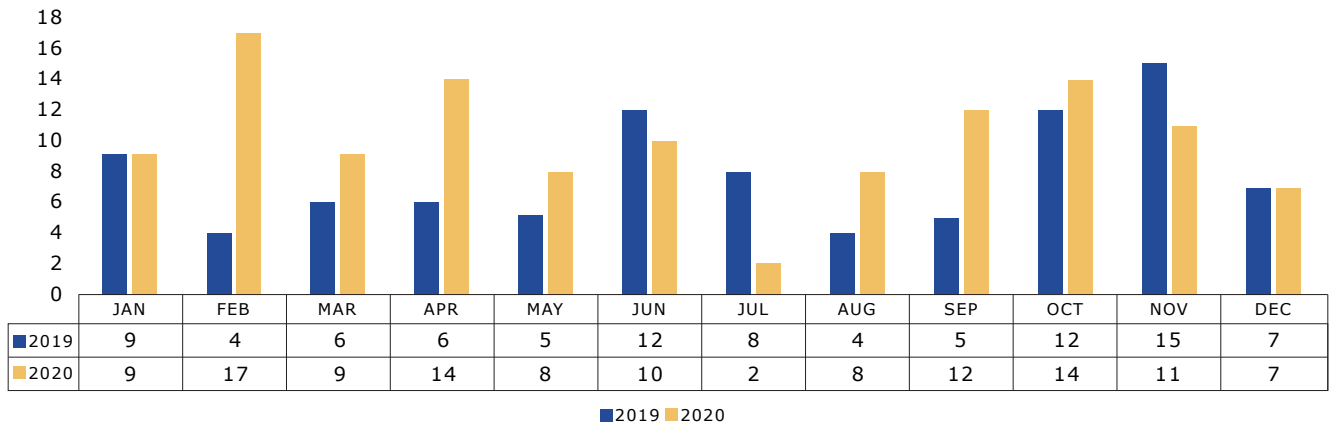


Figure 6 EDPS - Number of personal data breach notifications per month for the years 2019 and 2020

### Type of personal data breach notifications

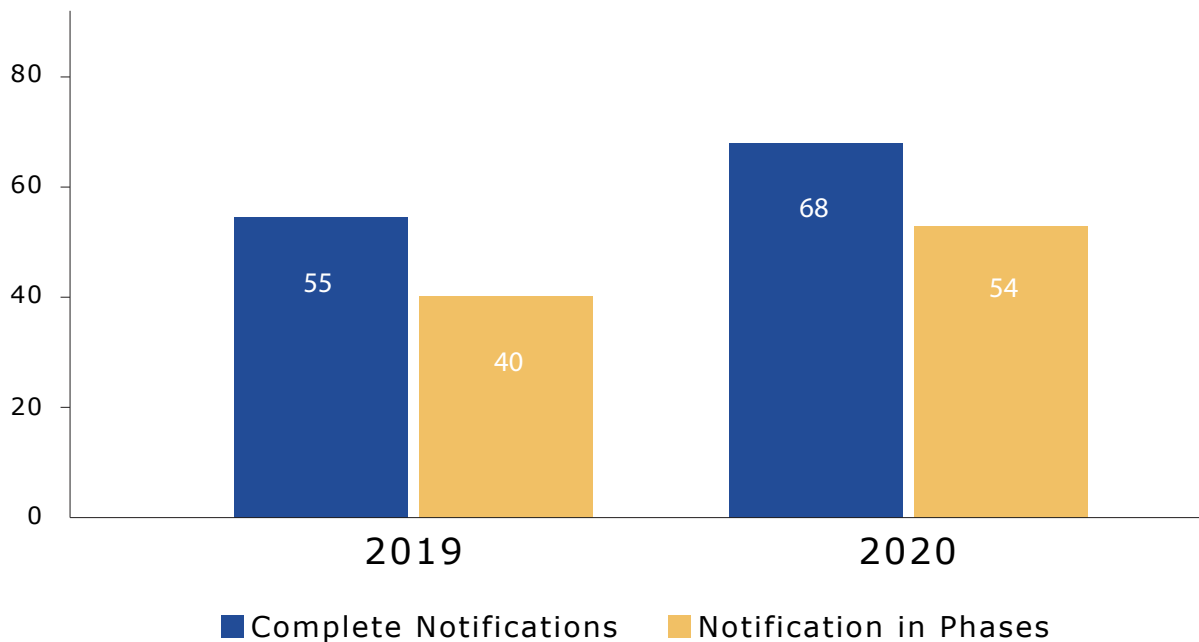


Figure 7. EDPS - Type of submission on personal data breach notifications in the year 2019 and 2020

### Type of Personal Data Breaches 2020

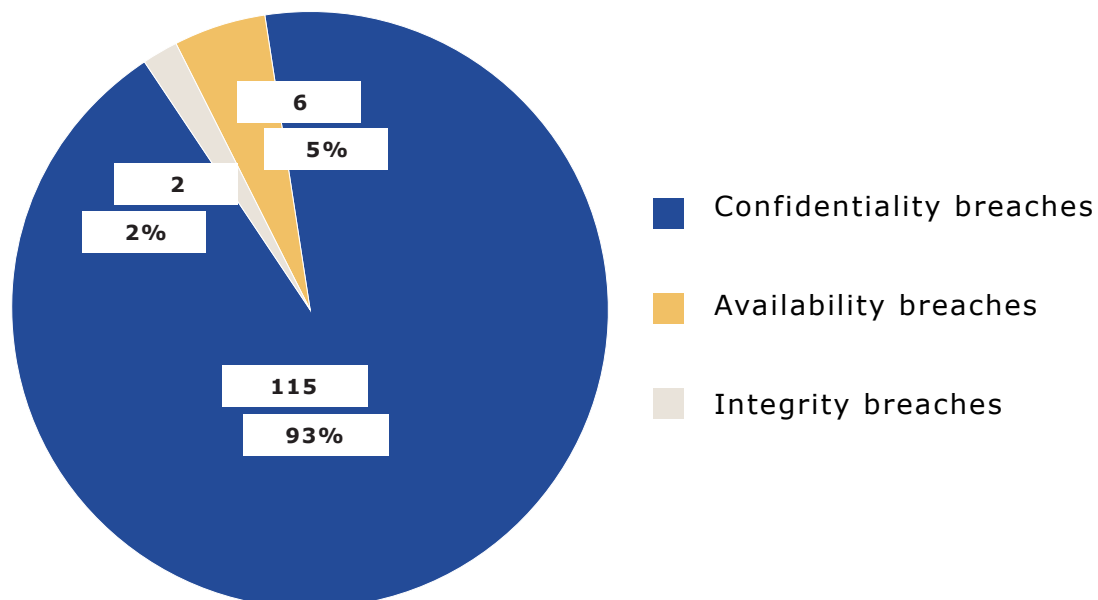


Figure 8. EDPS - Type of data breach notifications

### Type of Personal Data Breaches 2020

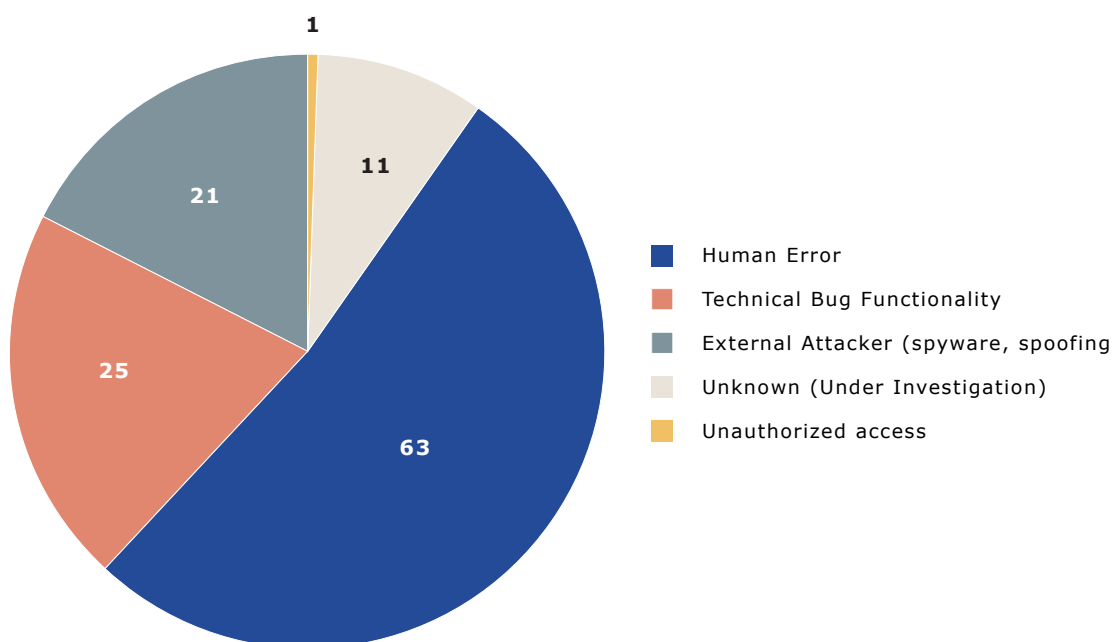


Figure 9. EDPS - Root cause of the personal data breach incidents



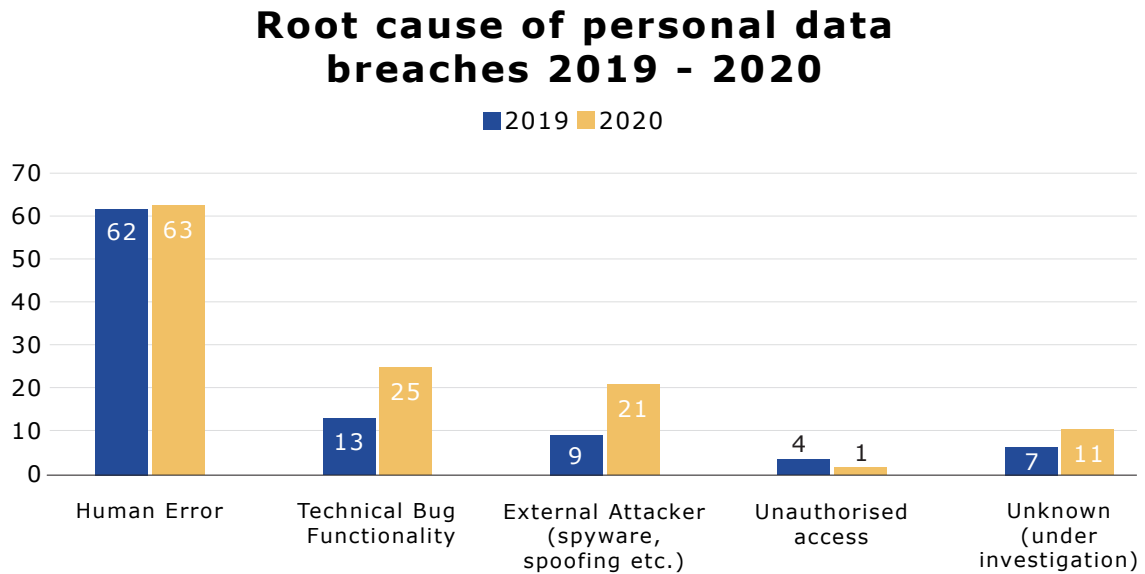


Figure 10. EDPS - Root cause of the personal data breach incidents - comparison 2019-2020

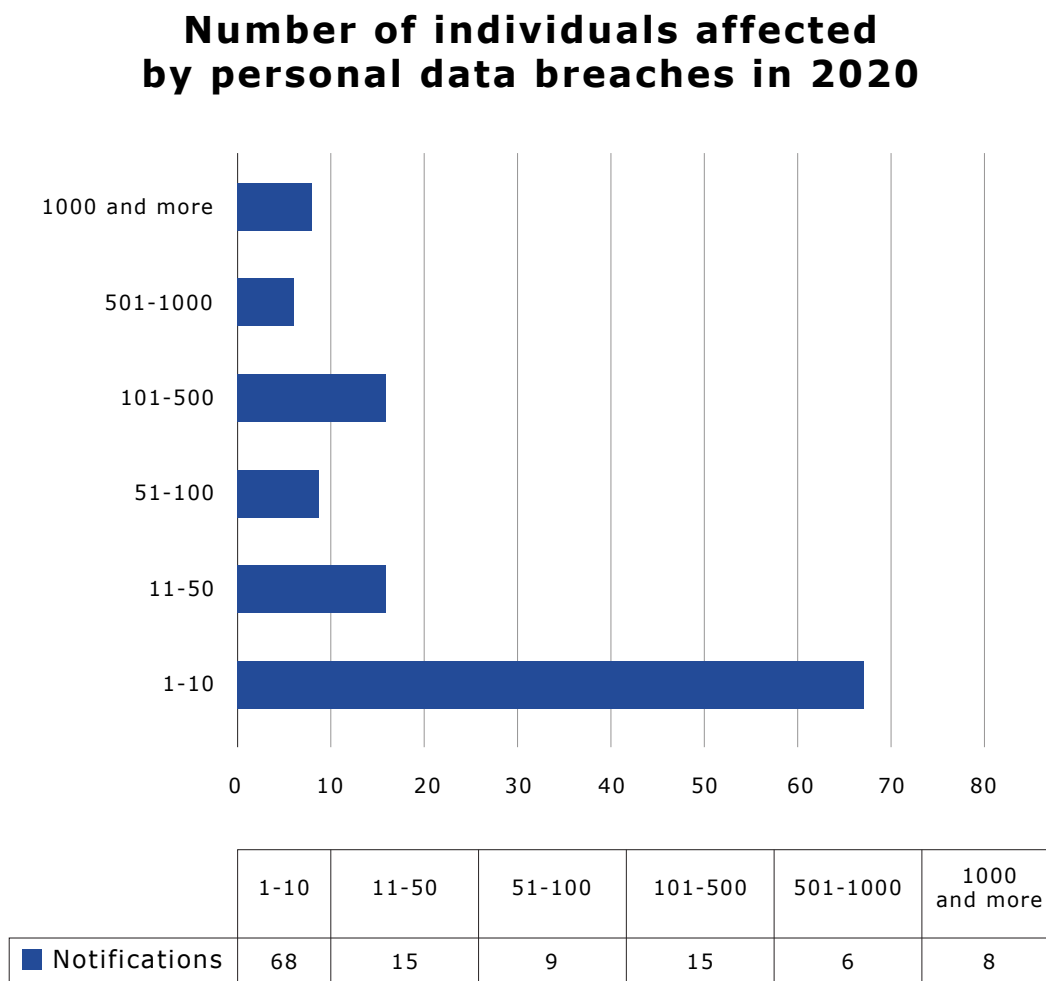


Figure 11. EDPS - Number of individuals affected by personal data breach incidents

### Communication to the data subject

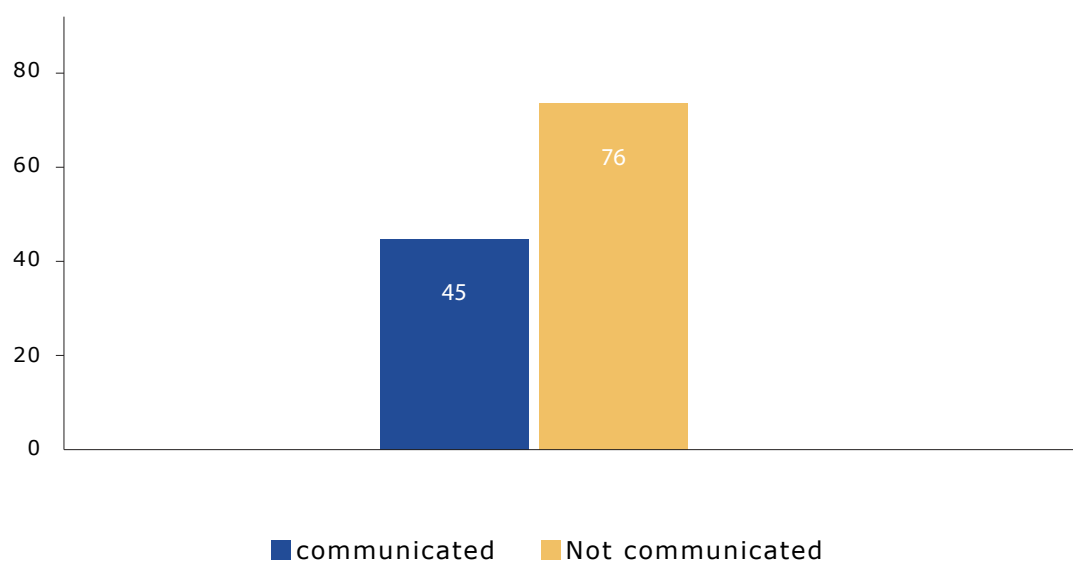


Figure 12. *EDPS - Number of personal data breach where the controller informed the data subject*

### Personal data breaches that affected special categories of data in 2020

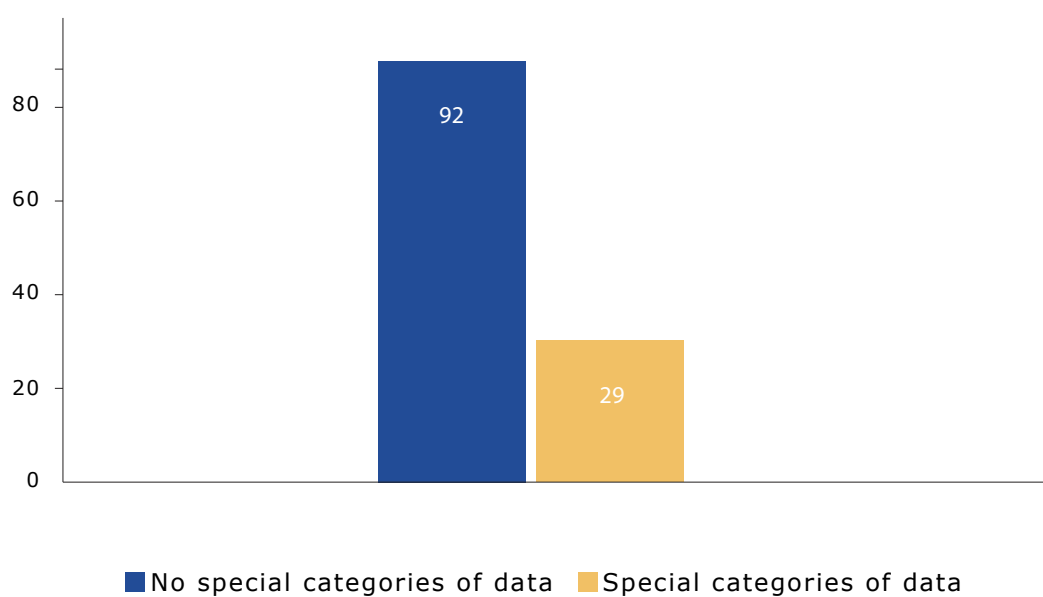


Figure 13. *EDPS - Special categories of data in personal data breach incidents*

## The Internet Privacy Engineering Network

The EDPS founded the [Internet Privacy Engineering Network \(IPEN\)](#) in 2014 to bring together experts from a range of different areas to encourage the development of engineering solutions to privacy problems. Through facilitating exchange between regulators, researchers and developers who build privacy into new and existing digital tools, IPEN aims to promote and advance state of the art practices in privacy engineering.

On 21 January 2020, we initiated an IPEN [panel](#) as a side event to one of the leading data protection and privacy conferences in Europe and around the world, the Computers, Privacy and Data Protection Conference (CPDP), to discuss increasingly pervasive and problematic web tracking. Web tracking is an issue tightly linked to technology, and new technologies are emerging to help identify and fight unlawful web tracking. This event highlighted the efforts of DPAs to increasingly enforce the relevant provisions of the General Data Protection Regulation (GDPR) and of the [ePrivacy Directive \(2002/58/EC\)](#), and of consumer protection organisations to use legal means to curb web tracking. As part of the answer, the event showcased the EDPS [Website Evidence Collector](#) tool, made publicly available by the EDPS.

On 3 June 2020, the EDPS organised the first online IPEN [workshop](#) to focus on the state of the art in encryption and its role for protection of privacy and personal data. On 24 June 2020, the EDPS also set up a webinar on the use of encryption for Privacy Enhancing Technologies (PETs) as a follow-up event. The common objective for both events was to add more technical knowledge and better understanding to the debates on privacy and encryption by promoting the understanding of already available technologies, as well as encouraging their development and use when processing personal data.

On 21 October 2020, the EDPS arranged an IPEN [webinar](#) on contact tracing apps as a large-scale exercise in privacy engineering. The event gathered contact tracing app developers, national data protection authorities and colleagues working in the field of data protection to share experiences,

challenges and learn about the day-to-day application of the legal obligations regarding data protection by design and by default.

The EDPS looks forward to engaging with IPEN in future events to ensure a stronger, collaborative and effective approach to privacy engineering in practice.

### 3.5.3 Artificial Intelligence and facial recognition

Artificial Intelligence (AI) is a reality and has woven its way into everyday life: navigation systems, spam filters, weather forecasts, to name a few. There have been significant advancements in the field of machine learning, a subset of AI. The machines learn due to the complex algorithms that allow them to analyse huge data sets and make predictions using this data. Along with enhancing the machines' skills, increasing amounts of data are being collected and information on human behaviour are being monitored; all of which present challenges for privacy and data protection.

On 23 January 2020, the EDPS organised a side event at the CPDP as a follow-up to the EDPS World Café on AI, which took place two days earlier. The common purpose for both EDPS events was to gather a variety of perspectives and ideas on how to prepare for the challenges of AI supervision and the role of DPAs in this regard.

On 13 February 2020, the EDPS organised a workshop to discuss the EU's approach to and the challenges and opportunities of AI and facial recognition applications. The high-level discussions at the workshop also contributed to the [EDPS Strategy 2020-2024](#) and our long-term view of global trends, such as the need to ensure the sustainable development of new technologies and the assessment of their potential impact on fundamental rights.

On 19 February 2020, as a first step towards an EU regulatory framework to address the human and ethical implications of AI, the European Commission published its [Communication - A](#)

[European strategy for data](#) and [White Paper on Artificial Intelligence - A European approach to excellence and trust](#). The EDPS [Opinion](#) presents our views on the White Paper as whole, as well as on certain aspects, such as the proposed risk-based approach, the enforcement of AI regulation and the specific requirements for remote biometric identification (including facial recognition). Our recommendations aim to clarify, and where necessary, further develop the safeguards and controls in regard to the protection of personal data.

### 3.5.4 The use of Microsoft by the EUIs

The EDPS carried out an own-initiative investigation into EUIs' use of Microsoft products and services and issued a [Public Paper](#) detailing our findings and recommendations. These findings may help any public administration in the EU when contracting IT services because of the extensive correspondence between the GDPR and Regulation (EU) 2018/1725, which applies to the EUIs.

Our Public Paper emphasises that when public administrations enter into contractual relationships with IT service providers, the terms of these contracts should reinforce the EUIs' control over how and why personal data is processed. To this end, the EUIs should properly embed data protection in each specific public IT procurement procedure, specifying the technical and organisational measures to ensure adequate level of security and data protection, in a way that those product and services can support compliance with the applicable Regulation and, in particular, the principle of data protection by design and by default.

Further information about the use of Microsoft by EUIs can be found in [section 3.2.2 of this Report](#).

### 3.5.5 The Hague Forum

The Hague Forum, jointly organised by the EDPS with the Dutch Ministry of Justice and Security and the European Commission, met for the second time on 2 July 2020. The Hague Forum is a cooperation platform for public authorities in the EU, EUIs and other international organisations to exchange

information and strengthen their negotiation power with IT service providers, including cloud service and communications providers. Sharing technical expertise and reinforcing regulatory cooperation among participants makes it possible to contribute to ensuring the same level of data protection safeguards and measures for all consumers and public authorities living and operating in the EEA.

During the July 2020 [event](#), the EDPS issued our Public Paper on EUIs' use of Microsoft products and services. The EDPS recommends that the roles and responsibilities of data processors and sub-processors should be clearly defined by the contractual agreements and monitored to minimise risks for the privacy of individuals.

Further information about the Hague Forum can be found in section 3.2.3 of this Report.

### 3.5.6 EDPS investigation into the 2019 European Parliament elections

As part of its campaign activities for the 2019 EU parliamentary elections, the European Parliament set up a website called [thistimeimvoting.eu](#) aimed at promoting public engagement. During the campaign, the website collected personal data from over 329,000 people, which was processed on behalf of the Parliament by an US political campaigning company, NationBuilder.

The EDPS visited the European Parliament in November 2019 to check its data retention procedures, and confirmed the deletion of data from over 260,000 users. In 2020, the EDPS closed its [investigation](#) into the European Parliament's use of NationBuilder, which resulted in the first EDPS reprimands issued to an EUI. The European Parliament responded by implementing EDPS recommendations, including informing individuals of their revised intention to retain personal data collected by the [thistimeimvoting.eu](#) website until 2024.

Cooperation and understanding between the EDPS and the European Parliament improved over the course of the investigation, culminating



in the end of the European Parliament's contract with NationBuilder and a commitment from the European Parliament to lead by example in the protection of personal data during the next EU Parliamentary elections campaign in 2024.

### 3.5.7 EDPS Orientations on body temperature checks

The EDPS published [Orientations on the use of body temperature checks by EUIs in the context of the COVID-19 pandemic](#). The EDPS notes that in compliance with [Article 24](#) of Regulation (EU) 2018/1725, temperature checks applied on a mandatory basis should not be based solely on automated processing.

We provided a non-exhaustive list of technical and organisational recommendations that should be duly taken into account to ensure that appropriate safeguards are in place, for example ensuring that systems for body temperature checks are done in real-time and not linked to other systems. We also outlined specific recommendations for transparency when it comes to informing any individual entering an EUI building that a temperature check system is in place, ensuring a suitable follow-up procedure in the event of a 'positive' temperature check, and continuously reviewing the necessity and proportionality of temperature checks.

### 3.5.8 Mobile apps and privacy

The EDPS is working on improving the capacities of its own technology lab to be able to audit mobile apps. To this end, an audit into mobile apps used by EUIs was initiated in December 2020.

The EDPS also wishes to closely collaborate with the EDPB to help other data protection officers (DPOs) with mobile app audits. Consequently, the EDPS organised a training session which brought together experts from four European DPOs. The EDPS continues to organise training sessions and raise awareness about the data protection concerns when EUIs use apps.

During training sessions for EUIs' DPOs, T&P provides an overview of how a mobile app is

developed, how individuals' data is collected when they are using a mobile app and the impact that this might have on individuals' right to data protection and privacy. Sessions also include group exercises for EUIs' DPOs to understand the issues at stake for their day-to-day work.

## 3.6 Legislative consultations

In addition to being responsible for monitoring the processing of personal data by EUIs, the EDPS also has the duty to advise the European Commission, the European Parliament and the Council on legislation and policy initiatives with impact on personal data protection.

Since [Regulation \(EU\) 2018/1725](#) entered into force in December 2018, the European Commission is obliged by law to consult the EDPS on all legislative proposals and international agreements which might have an impact on the processing of personal data. Such an obligation also applies to draft implementing and delegated acts (Article 42(1)).

According to [Article 42\(2\)](#) of Regulation (EU) 2018/1725, the Commission has the possibility to also consult the EDPB on proposals of "particular importance" for personal data protection. In such cases, the EDPS and EDPB work together to issue a joint opinion.

The statutory deadline for providing advice in the context of a legislative consultation is 8 weeks. In accordance with Article 20 of the [EDPS Rules of Procedure](#), the EDPS issues [Formal Comments](#) or [Opinions](#) in response to a request for legislative consultation.

According to Recital 60 of Regulation (EU) 2018/1725, the Commission should endeavour to consult the EDPS when preparing proposals or recommendations. We therefore remain available to be consulted informally by the Commission at an early stage of internal decision-making procedures, so as to be able to efficiently address any data protection issues. We respond to such consultation verbally or in writing, but do not publish our Informal Comments.

The EDPS meets annually with the legislative coordinators and Data Protection Coordinators from across the Commission to discuss the Commission Work Programme and identify initiatives likely to require consultation with the EDPS.

Finally, the EDPS may advise, on his or her own initiative or on request, all EU institutions and bodies on legislative proposals relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data. In such cases, we issue Comments or Opinions according to [Article 57\(1\)\(g\)](#) of Regulation (EU) 2018/1725.

### 3.6.1 Exchange of personal data between Europol and New Zealand's law enforcement authorities

On 31 January 2020, the EDPS adopted an [Opinion](#) on the negotiating mandate to conclude an international agreement on the transfer of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and New Zealand's law enforcement authorities.

The envisaged agreement aims to provide the legal basis for the transfer, as well as support and strengthened cooperation in preventing and combating serious transnational crime and terrorism whilst safeguarding data privacy and other fundamental individual rights and freedoms.

The EDPS notes that New Zealand has a well-established national data protection system in place, including a competent supervisory authority to oversee the work of law enforcement authorities. The EDPS appreciates that the Commission incorporated a number of specific recommendations from our [2018 Opinion](#) on international agreements permitting the exchange of data between Europol and non-EU countries into the proposed negotiating mandate with New Zealand.

The recommendations in Opinion 1/2020 focus on clarifying, and further developing where necessary, safeguards in the context of data protection transfers to New Zealand. In particular, we recommended focusing on purpose and storage limitation by

clearly specifying the criminal offences about which personal data can be exchanged and periodically reviewing the need for storage of that data.

The EDPS further recommends the need for clear and detailed rules on the right to information (such as how EU individuals may exercise their rights of access, erasure and rectification in New Zealand), and further information relating to the legal basis for the transfer of personal data.

### 3.6.2 Negotiating a new partnership with the UK

On 24 February 2020, the EDPS issued an [Opinion](#) on the Commission's recommendation to authorise the opening of negotiations for a new partnership with the United Kingdom (UK).

In our Opinion, the EDPS supports a partnership which affirms the EU and UK commitment to and respect for a high level of data protection and the EU data protection rules. The Opinion recommends:

- commitments to respect fundamental rights, including data protection, equivalent to those for the economy and security;
- defining priorities for international cooperation other than law enforcement, particularly between public authorities (including EUIs); and
- assessing transfers of personal data in the light of the CJEU [Opinion 1/15](#), for economic and security partnerships.

Given the aim of continued close cooperation at the end of the transition period, the EDPS welcomes the Commission's commitment to work towards the adoption of adequacy decisions, but highlights:

- the importance of an assessment of adequacy under the General Data Protection Regulation ([GDPR](#)) and Law Enforcement Directive ([LED](#)) for cooperation between public authorities and its impact on transfers by EUIs to the UK;
- the importance of defining the scope of adequacy decisions, particularly under the LED;



- that adequacy decisions are subject to specific conditions;
- the EDPB should be appropriately involved if the Commission presents a draft adequacy decision;
- any substantial deviation from EU data protection laws lowering the level of protection would obstruct an adequacy decision; and
- the EU should prepare for all eventualities, including where adequacy decision(s) cannot be adopted within the transition period or at all, or only for some areas.

### 3.6.3 Administrative cooperation in the field of taxation

On 28 October 2020, the EDPS issued an [Opinion](#) containing recommendations to minimise the impact upon the fundamental right to privacy by the Commission proposal amending [Directive 2011/16/EU](#) on administrative cooperation in the field of taxation.

The EDPS acknowledges that tax compliance is in the public interest, but insists on the right balance with privacy via an emphasis on data protection by design and by default, and data accuracy and minimisation in the context of automatic exchanges of data between national tax authorities.

The EDPS recommends that in respect of the management of the secure central interface on administrative cooperation on taxation:

- the Commission ensures that this management complies with the security provisions of Regulation (EU) 2018/1725, following our [Guidelines on the protection of personal data in IT governance and management of EUIs](#); and
- the Commission's role in respect of this management is ascertained in the context of any further arrangement with EU Member States and the technical and logistical support for the interface.

The EDPS stresses it expects to be consulted, according to [Article 42\(1\)](#) of Regulation (EU) 2018/1725, on the acts defining the administrative arrangements for technical and logistical support for the interface where Member States communicate via standard forms according to Directive 2011/16/EU, before their adoption.

As the competent supervisory authority under Regulation (EU) 2018/1725, the EDPS may follow up on updates concerning the interface and implications of the Commission's role within the processing operations in the context of administrative cooperation on taxation.

### 3.6.4 Combatting child sexual abuse online

On 11 November 2020, the EDPS issued [Opinion 7/2020](#) in relation to the Commission [Proposal](#) for a Regulation on a temporary derogation from certain provisions of the [ePrivacy Directive](#) (2002/58/EC). The Proposal relates to the voluntary use of technologies for combating child sexual abuse online.

The EDPS considers that the measures envisaged by the Proposal would constitute an interference with the fundamental rights of electronic communications service (for example, instant messaging) users with respect to their private life and data protection (in particular, confidentiality of their communications), which should only be possible under certain conditions. The issues at stake are not specific to the fight against child abuse, but to any initiative involving private sector collaboration for law enforcement purposes.

The EDPS stresses that measures to detect, remove and report child abuse must be accompanied by a comprehensive legal framework which meets the requirements of [Articles 7](#) and [8](#) of the Charter of Fundamental Rights of the EU.

Moreover, in order to satisfy the requirement of proportionality, the legislation must set clear and precise rules governing the scope and application of the relevant measures and imposing minimum safeguards to provide sufficient guarantees of the

protection of personal data against the risk of abuse. Our Opinion provides an overview of the necessary safeguards.

As the Proposal will serve as a precedent, the EDPS considers it essential that it is not adopted, even as a temporary derogation, until all the necessary safeguards set out in our Opinion are integrated.

### 3.6.5 A new pact on migration and asylum

In light of the proposals presented in the [New Pact on Migration and Asylum](#) by the European Commission, the EDPS issued an [Opinion](#) on 30 November 2020.

The European Asylum Dactyloscopy Database ([EURODAC](#)) is an EU database that identifies asylum seekers applying for international protection by collecting their fingerprint data. A proposed amendment concerns the Regulation applicable to EURODAC, by implying the automatic linking of all data corresponding to the same third-country national in a “sequence”. This amendment would potentially broaden EU Member States’ and authorities’ access to sensitive data irrelevant to asylum.

The EDPS understands the need for more effective management of asylum and migration, but recommends:

- as per the recommendations under [Opinion 07/2016](#) on the reform package on the Common European Asylum System, a fundamental rights and data protection impact assessment should be carried out for this envisaged amendment;
- EU Member States and their authorities should continue to only be able to see the data that is relevant for the performance of their tasks, even if the datasets are linked in a sequence;

and that the Commission:

- clarifies the type of data stored in EURODAC in line with the data protection principles of necessity and proportionality;

- updates the EURODAC security infrastructure with appropriate data protection safeguards; and
- introduces the single model of coordinated supervision.

On the proposal for a Screening Regulation to collect data on the identity, health and security checks of third-country nationals, the EDPS advises the Commission to evaluate their method of collecting and processing this data. This would mean accounting for national practices featuring different levels of efficacy, ensuring data accuracy and upholding data subjects’ right to rectification.

### 3.6.6 Highlights from the Formal Comments on large-scale database systems in the area of Justice and Home Affairs

The EU large-scale database systems in the area of Justice and Home Affairs operate under a complex legal framework, characterised by many wide ranging implementing and delegated acts. Such complexity is further increased by the establishment of a framework that aims to make these systems interoperable, further amplifying the impact on the right to the protection of personal data. As these systems are interconnected, there is a need to make very clear the purpose, the legal basis and the rules and responsibilities of those involved to ensure that individuals’ personal data is protected.

In this context, the EDPS issued a number of [Formal Comments giving advice on technical matters as well as more general principles of EU law pertinent to data protection](#). The examples provided here focus on some of the Formal Comments the EDPS issued on the Schengen Information System (SIS II), European Travel Information and Authorisation System (ETIAS) and Entry / Exit System (EES).

Examples of Formal Comments on a number of other matters issued by the EDPS in 2020 are also presented here. A complete list of Formal Comments can be found in [Annex D](#).



### Formal Comments related to the Schengen Information System

SIS II contains alerts on individuals and objects entered by the competent national authorities with the purpose of locating those individuals or objects in another EU Member State and taking a specific action.

On 26 August 2020, the EDPS issued [Formal Comments](#) on the Commission's two draft Implementing Decisions on the minimum data quality standards and technical specifications for the processing of biometric data in the SIS II. As a general remark, the EDPS reiterates its previous recommendations issued in Opinion 07/2017, highlighting that the necessity to use biometric identifiers should be demonstrated and that DNA profiles introduced in SIS should contain only the minimum information that is strictly necessary for the identification of the missing individual, excluding explicitly health information, racial origin and any other sensitive information.

The EDPS has concerns that the Decisions provide very limited detail regarding the minimum data quality standards and technical specifications of the biometric identifiers in SIS II, in particular regarding the thresholds for entering, storing and searching biometric data in the Technical Specifications and the SIS II Interface Control Document. The EDPS recommends that the Document, even if developed by the EU agency for the Operational Management of Large-Scale IT Systems in the AFSJ ([eu-LISA](#)) due to their specific knowledge and expertise, should be either formally adopted or at least reviewed and officially approved by the Commission. The same approach should apply to any subsequent amendment of the Document.

### Formal Comments related to the Schengen Information System

On 26 August 2020, the EDPS also issued [Formal Comments](#) on the Commission's two draft Implementing Decisions on the technical rules necessary for entering, updating, deleting and searching data in the SIS II.

The EDPS welcomes the introduction in the Decisions of specific measures and tools aimed at ensuring high quality of the data entered in SIS II, in line with principle of data accuracy and to help prevent errors with potentially serious negative consequences for the affected individuals and their personal data. We positively note the attention paid to the requirement for explicit consent of an individual, whose identity has been misused, for entering additional data about them in SIS II.

The EDPS expressed concerns about legal competence and allocation of responsibility concerning the sub-delegation of powers by the Commission to eu-LISA. The EDPS underlines that eu-LISA should only perform the tasks conferred to them by the respective legal basis of SIS II. The EDPS further highlights that the legal framework should be interpreted in light of the jurisprudence of the CJEU, according to which no discretionary power may be delegated. The EDPS also reiterates its recommendation for the Commission to formally approve adoption and amendment of the Technical Specifications and SIS II Interface Control Document.

### Formal Comments on ETIAS

Regulation (EU) 2018/1240 established the European Travel Information and Authorisation System ([ETIAS](#)) for third-country nationals exempt from the requirement to be in possession of a visa when crossing the external borders and laid down the conditions and procedures for issuing or refusing a travel authorisation. More specifically, ETIAS requires visa-exempt third country nationals, seeking to enter the EU, to undergo a risk assessment concerning security, irregular migration and public health risks prior to their arrival, via the crosschecking of their personal data (that they submit in an online application) against other EU systems such as SIS II, a dedicated ETIAS watch list established by Europol, and ETIAS screening rules.

The EDPS issued Formal Comments on the Commission's Implementing Decision on the rules on the operation of and on data protection and security applicable to the ETIAS public website and app for mobile devices. In particular, the EDPS highlights that the detailed rules should be based

on information security risk management and on principles of data protection by design and by default.

The EDPS further issued Formal Comments on the Commission's draft Implementing Decision on defining the requirements concerning the format of the personal data to be inserted in the ETIAS application form, as well as the parameters and verifications to be implemented for ensuring the completeness of the application and the coherence of this data.

### The Commission's new Entry/Exit System website

On 1 October 2020, the EDPS issued Formal Comments on the Commission's draft Implementing Decision related to specific conditions for the Entry/Exit System (EES) website.

The EES was established by [Regulation \(EU\) 2017/2226](#) to register entry and exit data, including information on the refusal of entry of third country nationals who applied for a short stay in the Schengen area.

Third country nationals should be notified of the purpose of EES, how their personal data will be handled and how they can access this data. To make third country nationals aware of their rights regarding their personal data, the Commission should set-up a website containing this information.

The public website should gather in a single place the information about the EES and provide access to the functionalities of the EES. This includes, for example, web service to verify the remaining authorised stay and a functionality allowing third country nationals to contact the appropriate authorities of the country where they would like to make use of their rights related to data protection.

Taking into account the above-mentioned context, key recommendations of the EDPS included:

- defining the roles of data controller and processor;
- outlining who should access the logging information of the website and for what purpose(s);
- clarifying whether the intention is to develop a mobile app in addition to the website and if so, under which legal basis; and
- defining what type of tracking technology will be used.

The EDPS will continue to assist and advise on the data privacy and security implications that the development of the EES website entails.

### 3.6.7 Other Formal Comments

On 3 July 2020, the EDPS issued [Formal Comments](#) highlighting the lack of safeguards for EU data protection law within Frontex's draft working arrangements with third countries. The EDPS makes recommendations on individuals' data privacy rights, and emphasised that sensitive data exchanges between Frontex and third countries may require additional security measures or be subject to restrictions (for example, under [Article 90 of the EBGC Regulation](#) data processed by Frontex to identify cross-border crime suspects can only be exchanged with Europol, Eurojust or Member States' competent authorities). The EDPS underlines the importance of redress mechanisms where judicial remedies are unavailable in a third country, and how independent oversight can guarantee that the country in question and Frontex comply with specific provisions in a working arrangement.

On 28 August 2020, the EDPS issued [Formal Comments](#) on the draft Delegated Regulation and the draft Implementing Regulation relating to the optional common EU scheme for rating buildings' smart readiness. In this regard, the EDPS recommends a prior assessment of cybersecurity and privacy threats, in line with privacy by design and default principles, to identify, address and inform users about relevant data protection risks before using 'smart-ready' services or technology. The EDPS underlines that the proposed regulation should ensure a high level of protection of



personal data, delineating the purpose, type and nature of data being processed, particularly when incorporating home automation systems.

On 31 August 2020, the EDPS issued [Formal Comments](#) to welcome the approach of the Implementing Regulation to harmonise and update data requirements of customs declarations and notification in the Union Custom Code (UCC), simplifying movement of goods in and outside the EU. The EDPS notes that customs authorities and economic operators exchange and store names of legal persons which can amount to personal data if they identify natural persons. In its Formal Comments, the EDPS highlights that the draft Delegated Regulation entails processing of limited categories of personal data for the performance of the customs declaration obligations pursuant to the UCC, and does not raise data protection issues meriting specific recommendations.

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

The [European Data Protection Board](#) (EDPB) is an independent body established under the [General Data Protection Regulation](#) (GDPR) that promotes cooperation between national 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, which offers administrative and logistic support, performs analytical work and contributes to the EDPB's tasks. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPS and the EDPB.

#### 3.7.1 Support Pool of Experts

On 24 June 2020, the EDPS published a [Press Release](#) welcoming the European Commission's first review of the GDPR, which emphasises that the consistent and efficient enforcement of the GDPR remains a priority.

To this end, in July 2020, the EDPS proposed the establishment of a Support Pool of Experts (SPE) within the EDPB, to assist DPAs in their complex

tasks. The EDPS, together with the EDPB Secretariat and other EDPB members, developed [terms of reference](#) with a view to preparing a pilot project in 2021, which will serve as a basis for establishing the SPE, as outlined in the [EDPB Strategy 2021-2023](#). 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.

The EDPS also contributed to the drafting of the [Recommendations](#) on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and the [Recommendations](#) on the European Essential Guarantees for surveillance measures, published on 10 November 2020. These documents were adopted after the "Schrems II" ruling to ensure ongoing and future international data transfers are carried out in accordance with EU data protection law. The EDPS and EDPB will continue to work collaboratively to protect individuals' personal data throughout the EU / EEA.

#### 3.7.2 Cooperation in the framework of the EDPB

Established under the GDPR, the EDPB replaces the [Article 29 Working Party](#) as the forum for cooperation between the DPAs of the European Economic Area (EEA) and the EDPS. It also takes on many new tasks, aimed at ensuring the consistent application of the GDPR across the EEA. In addition to this, the EDPB is able to issue decisions, Opinions, guidelines and statements on a wide range of topics.

Under the new legal framework, the EDPS is tasked with providing the secretariat for the EDPB. In addition to providing the secretariat, the EDPS is a full member of the EDPB and attended the 27 EDPB plenary meetings, which took place in 2020.

Much of the work carried out by the EDPB takes place within expert subgroups, each relating to a specific area connected to data protection. These include key provisions of the GDPR, international transfers, technology and financial matters, among many others.

As a member of the EDPB, we contributed actively, as rapporteurs or co-rapporteurs, to several key initiatives of the EDPB in 2020, such as:

- EDPB cooperation with the European Commission in the context of its initial and in-depth investigation of the proposed Google-Fitbit merger;
- [Guidelines](#) on the concept of relevant and reasoned objection;
- a statement and a FAQ on the “[Schrems II](#)” [ruling](#) providing first answers on the impact of the decision;
- [Guidelines](#) on Connected Vehicles;
- the first binding EDPB decision on the basis of Article 65 of the GDPR, which concerns a draft decision by the Irish DPA on Twitter International Company;
- [Guidelines](#) on the processing of Personal Data through Video Devices;
- The [EDPB Strategy 2021-2023](#), which sets out the EDPB’s strategic objectives, grouped around four pillars, as well as three key actions per pillar to help achieve these objectives;
- [Guidelines](#) on the concepts of controller and processor in the GDPR;
- a Statement on privacy implications of mergers;
- the EDPB [contribution](#) to the evaluation and review of the GDPR under Article 97 of the GDPR;
- [Guidelines](#) on transfers between public authorities;
- [Guidelines](#) on the processing of health data for research purposes in the context of the COVID-19 outbreak;
- [Guidelines](#) on geolocation and other tracing tools in the context of the COVID-19 outbreak;
- a letter regarding the Polish presidential elections taking place via postal vote;
- a statement on data subject rights in connection to the state of emergency in Member States and a letter regarding the Hungarian Government’s Decree 179/2020;
- an opinion on the draft Standard Contractual Clauses (SCCs) for controller-processor contracts submitted to the EDPB by the Slovenian DPA;
- a statement on the interoperability of contact tracing applications and a statement on the processing of personal data in the context of reopening the Schengen borders following the COVID-19 outbreak;
- the publication of a new register containing decisions taken by national DPAs following the One-Stop-Shop cooperation procedure (Article 60 of the GDPR);
- [Recommendations](#) 1/2020 on supplementary measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data;
- [Guidelines](#) on the targeting of social media users;
- the final version of the Guidelines on Data Protection by Design & Default (after public consultation);
- the setting up of a Coordinated Enforcement Framework, which provides a structure for coordinating recurring annual activities by DPAs;
- the [Guidelines](#) on restrictions of data subject rights under Article 23 of the GDPR;
- the establishment of a Support Pool of Experts (SPE) on the basis of a pilot project. The goal is to provide material support to EDPB Members in the form of expertise that is useful for investigations and enforcement activities and to enhance cooperation and solidarity between EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs; and
- the final version of the Guidelines on the interplay of the Second Payment Services Directive (PSD2) and the GDPR.

### 3.8 International Cooperation

As data flows across borders, there is a need to consider data protection in a [global context](#).

The EDPS actively participates in a number of international fora with the aim of:

- sharing information and good practices;
- finding common positions and developing guidance; and
- working together to improve the understanding of data protection law.

#### 3.8.1 The Global Privacy Assembly

The EDPS is an active member of the Global Privacy Assembly (GPA) (previously known as the International Conference of Data Protection and Privacy Commissioners, ICDPPC) and former host of the 2018 Conference that gathered more than 1000 delegates discussing digital ethics and the challenges of a data driven society.

For more than four decades, the GPA has been the premier global forum for data protection and privacy authorities providing leadership at international level and connecting the efforts of more than 130 DPAs from across the globe. The Assembly supports Working Groups in the fields of international enforcement and cooperation, policy standards, consumer protection, digital economy and ethics among others.

The 2020 Closed Session of the GPA took place remotely, due to the COVID-19 pandemic, from 13 to 15 October 2020.

The Assembly started by providing a follow-up to the work performed in the context of the GPA Policy Strategy, based on the three pillars of:

- advancing global privacy in a digital age, confirming a move towards a global regulatory environment;
- maximising the conference's voice and influence, notably in enhancing the conference's role in

digital policy and strengthening relationships with other international bodies and networks. The update on this pillar was provided by the EDPS, as chair of this working group; and

- capacity building to support members sharing expertise year-round.

Moreover, the chairs of the various GPA Working Groups provided an overview of the work and activities performed throughout the year. In this context, the EDPS, in its role as co-chair, also presented the Working Group on Data Protection and Ethics in Artificial Intelligence.

The Closed Session included a detailed discussion on data protection and privacy in the context of the COVID-19 pandemic, and produced five new [resolutions](#):

- on Facial Recognition Technology;
- on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management;
- on Accountability in the Development and Use of Artificial Intelligence;
- on the Privacy and Data Protection challenges arising from the COVID-19 pandemic; and
- on Joint Statement on Emerging Global Issues.

The next edition of the conference will take place in October 2021 in Mexico City (Mexico), if the circumstances will allow in-person conferences.

#### 3.8.2 International organisations workshop

Generating and fostering global partnerships in the field of data protection has always been one of the priorities 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 the 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 demonstrates the increasing awareness of the importance of ensuring strong safeguards for personal data.

The most recent workshop was a markedly different event than in previous years. The continuing global health crisis prevented an in-person workshop, so the EDPS hosted a shorter online workshop on the afternoons of 8 and 9 October 2020. In light of the COVID-19 pandemic, the theme of this online workshop was ‘Data Protection in International Organisations in Times of Crisis’. There was a definite appetite for the workshop and the theme, with over 140 participants from international organisations engaging in the discussions. To help facilitate an overview of the state of play of data protection within international organisations, distinguished speakers – experts and academics from Europe and beyond, as well as colleagues from the EDPS – gave presentations on a number of pertinent subjects. Topics discussed over the two afternoons included the impact of the pandemic for the protection of personal health data in a humanitarian context, remote working, contact tracing apps, level of preparedness and lessons learned during the pandemic and new developments and best practice to facilitate transfers to international organisations.

### 3.8.3 Council of Europe

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+](#), was the first legally binding international instrument in the field of data protection.

Any country can sign up to the Convention, with 55 countries now party to it and its additional Protocol regarding DPAs 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 safeguards. The modernised

[Convention 108](#) was opened for signature on 10 October 2018.

The EDPS participates in the Council of Europe’s expert groups on data protection, such as the Consultative Committee (T-PD) of Convention 108, as an observer. Our role involves ensuring a high standard of data protection and compatibility with EU data protection standards. Topics of great interest are currently on the agenda of the T-PD: the evaluation and follow-up mechanism under Convention 108+, facial recognition, update of a recommendation on profiling, challenges in the context of educational systems, transborder access to personal data by law enforcement authorities, and personal data processing by and for political campaigns, etc.

As of March 2019, the EDPS also represents the GPA in the T-PD.

## 3.9 Cooperation with Civil Society

On 21 January 2020, the [Privacy Camp](#) hosted the European Data Protection Supervisor (EDPS) Civil Society Summit. This annual meeting between the EDPS and civil society organisations aims for the attendees to discuss the state of data protection and privacy in the EU. This year’s edition gave participants the opportunity to debate the rising threat of facial recognition. Members of the [EDRi network](#) and beyond took part in round-table discussions about the violations of the principles of proportionality and necessity, and other individuals’ rights that are impacted. Examples included the deployment of facial surveillance systems in France, Serbia and Wales.

The summit allowed participants to debate the merits of a ban on facial surveillance compared to the benefits of a temporary prohibition of the aforementioned. Discussions also touched on whether civil society should focus on improving the enforcement of existing legislation instead. During the summit, participants were also given the opportunity to consider the nuances between different circumstances in which facial recognition can be used, for example, whether it can be used in



public spaces or not.

The round-table discussions concluded with a nod to the old CCTV privacy/security debates. During these debates, participants recognised that the current approach to facial recognition is very fractured across EU Member States. In particular, the EDPS recommended civil society not to focus on the accuracy question, but, instead, to look at tools to address the risks for individuals' fundamental rights, using, for example, impact assessments.

## TRANSPARENCY AND ACCESS DOCUMENTS

As an EUI and according to our [Rules of Procedure](#), the EDPS is subject to [Regulation \(EC\) 1049/2001](#) on public access to documents. Within the EDPS, the person responsible for handling these requests is a designated legal officer. In order to meet the ever-growing demand for access to documents and to establish coherent policy and practices on the matter, the EDPS created the permanent position of Transparency Officer in October 2020. The appointed officer collaborates with the relevant staff members in order to respond appropriately to the requests.

In addition, in order to improve our work in the field of transparency we have started a review of the internal rules and procedure governing the access to documents. The process will finish in April 2021.

In 2020, the EDPS received 18 access to documents requests. In one of these cases, we also received a confirmatory application. In all cases where documents could be identified, the requested documents were either fully or partially disclosed.

All other transparency and communication actions are available on our 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 register in particular, with relevant documents and information on a regular basis.



## THE SECRETARIAT

### 5.1 Information and Communication

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 team aims to, therefore, ensure that EDPS activities and messages reach the relevant audiences at the right time.

The role of the team, reinforced in the [EDPS Strategy 2020-2024](#), 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's day-to-day work in clear language and via appropriate communication tools.

During the COVID-19 pandemic, it has been of particular importance to adapt and continue to strengthen the EDPS' online presence in order to fully connect with the relevant audience and stakeholders. The team's efforts focused on, but were not limited to, promoting the EDPS' COVID-19 pandemic actions as well as the EDPS Strategy

2020-2024, which highlights the EDPS' principles and strategic objectives for the next 4 years.

#### 5.1.1 Online media

##### Website

Alongside the more traditional publications available on the EDPS website, we decided to create a [dedicated website](#) to present the EDPS Strategy 2020-2024 in an interactive way to make it more appealing and accessible to a wider audience. As such, we chose a format and layout which allow visitors to easily navigate between our three strategic pillars and to quickly find the information they need.

The website includes extracts from our three strategic pillars, relevant videos, and the Supervisor's foreword summarising the most important points, so that visitors are able to gain an immediate understanding of the Strategy. There are additional short summaries and video's to inform visitors of relevant updates.

Visitors have the opportunity to find out more about the Strategy on our main website as well.

The EDPS launched our main [website](#) in 2017. Since then, we have continued to make improvements to it by adding new features and enhancing its design,

in response to our visitors' feedback and needs.

In September 2020, we created a [Frequently Asked Questions \(FAQ\)](#) webpage in order to provide readily accessible summaries of the EDPS' mission, powers, role and values. In response to the COVID-19 outbreak and in correlation with the creation of the EDPS COVID-19 task force, we set up a dedicated [webpage](#) highlighting our latest data protection work in this area. This webpage also includes information about the adoption of the European Data Protection Board's (EDPB) activities and resolutions at the Global Privacy Assembly (GPA).

We have started to migrate our website to DRUPAL 8, which will be completed in 2021. The EDPS developed a new visual identity towards the end of 2020, which will be reflected in the revamp of our website in 2021.

### EDPS blog

The [EDPS blog](#) is a platform through which the European Data Protection Supervisor Wojciech Wiewiórowski, the Director and, more recently, the 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. It has now been active for over four years and has established itself as an essential EDPS communication tool. The blog is easily found on the homepage of our main website where a short extract from the most recent blogpost is always displayed.

In 2020, the EDPS published 16 blogposts focusing on a range of different subjects. This has allowed us to share our analysis on upcoming technologies, in particular their potential, opportunities and prospective impact on data protection. Our blog has also been a beneficial outlet for the reporting of Data Protection Officers' (DPOs) networking events, other external events, EDPS organised workshop's such as the Internet Privacy Engineering Network (IPEN), and our yearly EDPS / EDPB trainee conferences. In the unprecedented circumstances of the COVID-19 pandemic, the EDPS blog has also been an opportunity for the Supervisor to convey messages of hope, strength and European solidarity.

### Social media

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

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. The [LinkedIn](#) platform allows the EDPS to communicate in a more detailed way with data protection specialists and actors in the field.

In 2020, we used our [YouTube](#) channel to share short videos explaining the EDPS Strategy 2020-2024 and to give visibility to our EDPS colleagues who are contributing to achieving our strategic objectives. The EDPS continues to use YouTube to post footage from various events that we have organised, publish informational videos on data protection principles (for example, a video explaining the use of Data Protection Impact Assessments [DPIAs] in July 2020) and broadcast some of the Supervisor's more important speeches and remarks.

The EDPS communication campaigns have been crucial for us to continue our interaction with our audience and stakeholders. Examples include, but are not limited to:

- **#ShapingSaferDigitalFuture** to promote specific aspects of the EDPS Strategy 2020-2024 over 6 weeks via videos on our social media platforms;
- **#StayAtHome** in response to the COVID-19 pandemic to encourage our audience to stay at home and limit the spread of COVID-19 by sharing EDPS colleagues' book recommendations;
- as we continue to welcome new followers in our ever-growing social media community, **#InCaseYouMissedIt** and **#LookingBackOn2020** are examples of campaigns we run twice a year to raise awareness of less high-profile topics, inform

DPOs, controllers and processors of their obligations by promoting our factsheets and guidelines; and

- **#CelebratingEU** to inform our audience about the role and cooperation of national DPAs with each other and the EDPS.

### 5.1.2 Events and publications

June 2020 marked the publication of the EDPS Strategy 2020-2024, setting the tone for the next 4 years to come. We postponed the launch of the Strategy in order to review it and reflect on the challenges posed by the COVID-19 pandemic. The 2020-2024 Strategy sets out a detailed plan of action to appropriately respond to the impact of this global health crisis on data protection.

It is also in this context that the EDPS has had to rethink the format of hosting events, switching to webinars and online workshops. This presented us with some challenges as well as opportunities to innovate.

#### Presentation of the EDPS Strategy 2020-2024

To mark the beginning of our new mandate on 30 June 2020, we invited over 200 stakeholders to the launch of the [EDPS Strategy 2020-2024](#). The audience was made up of people from the private and public sector, including European institutions, bodies and agencies (EUIs), academics and civil society. Following speeches from Supervisor Wojciech Wiewiórowski, Chairwoman of the EDPB Andrea Jelinek and European Commissioner for Justice Didier Reynders, there was also a lively Q&A session with many questions for the Supervisor about the Strategy.

#### The EDPS and the EDPB trainees' first online conference

On 7 July 2020, the EDPS and EDPB trainees organised a conference, in line with a long-established tradition marking the end of the cohort's blue book traineeship (a scheme which runs twice a year). This event, which focused on [Data Protection](#)

[in the Age of COVID-19](#), was held online for the first time due to the pandemic.

A range of data protection experts from academia, business, civil society and regulatory backgrounds, addressed the following questions:

- Yesterday: is the existing data protection framework robust and comprehensive enough to protect our rights before and during the global pandemic?
- Today: to what extent are the responses to the crisis balance against the right to data protection?
- Tomorrow: will the pandemic have a lasting effect on the perspective that society has on data protection?

Supervisor Wojciech Wiewiórowski and Head of the Secretariat of the EDPB, Isabelle Vereecken, made the opening and closing [remarks](#).

### Europe Day

Saturday 9 May 2020 marked the 70th anniversary of the 'Schuman Declaration'. At a speech in Paris in 1950, Robert Schuman, the then French Minister of Foreign Affairs, set out his idea for a new form of political cooperation in Europe, which would make war between Europe's nations unthinkable. Schuman's proposal is considered to be the beginning of what is now the European Union (EU) and so 9 May is also known as Europe Day.

This year, due to the COVID-19 pandemic, the EDPS, like all the EUIs, was unable to showcase the work it does or interact with the public on our physical stand at the EU Open Day as in past years. Instead, to commemorate Europe Day and to highlight the importance of the right to data protection even in times of crisis, we organised an online quiz for the general public to take part in.

### Celebrating Data Protection Day 2020

On 28 January 2020, we celebrated the 14th annual Data Protection Day ([DPD](#)). DPD marks the

anniversary of the Council of Europe's Convention 108, the first legally binding international framework for data protection. DPD 2020 was all the more special, as Europe also celebrated its Data Protection Golden Anniversary - 50 years since the first European data protection law was passed in the German Federal State of Hesse.

As has become the tradition, the EDPS and the EDPB marked DPD by participating in and setting up a number of the panels at the 2020 Computers, Privacy and Data Protection Conference ([CPDP](#)) (see section on [International conferences and workshops](#) of this Chapter), and organising a [conference](#) for EUI trainees. The latter conference explored:

- how individuals can develop a transparent and fully-functioning relationship with their personal data; and
- “data doubles”, the digital imprints individuals actively or passively create online, which are consequently used to categorise and target them, lingering throughout their lifetime and beyond.

EDPS Supervisor Wojciech Wiewiórowski and Head of the EDPB secretariat made presentations.

### Communicating with DPOs: Factsheets and infographics

The EDPS has published a series of factsheets, flowcharts, infographics and quick-guides in 2020 to provide information and support to DPOs, data controllers and processors, on various aspects of [Regulation \(EU\) 2018/1725](#). We use these communication tools with the aim to deliver complex information in a comprehensive and transparent way and, therefore, offer practical support with the aim to help EUIs with the consistent application of data protection laws in the EUIs. Some of the subjects that we have covered include administrative fines and our enforcement powers under Regulation (EU) 2018/1725, DPIAs, international transfers of personal data, duties of data controllers and processors, necessity and proportionality.



### EDPS Newsletter

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 matters of data protection.

In 2020, we published 9 newsletters to keep our audience up to date on EDPS activities in an approachable, condensed and informative way. These newsletters featured a wide range of topics, such as Artificial Intelligence (AI), complaints submitted against EUIs, international transfers of personal data and EPDS events and training sessions.

## 5.1.3 External relations

### Media relations

The EDPS issued 11 [press releases](#) and statements in 2020. All of our press releases are published on the EDPS and [EU Newsroom](#) websites, distributed to our network of journalists and other interested parties. We issued press releases on important data protection developments and activities that the EDPS has contributed to, such as the outcome of investigations, [Opinions](#) and reports. In particular, press releases have been a useful tool in 2020 to update our audience on our activities regarding international transfers of personal data, data protection issues related to COVID-19, for example.

In addition to our press releases, we received 84 formal requests from European and international



press on a wide variety of topics. Activities on which we garnered a considerable degree of press attention included the EDPS Strategy 2020-2024, our Strategy for EUIs to comply with the “Schrems II” ruling, the outcome of own-initiative investigation into EU institutions’ use of Microsoft products and services, our Opinion on combating child sexual abuse online, the interplay between data protection and scientific research, issues (mainly enforcement) under the GDPR, as well as our supervision and admonishment of Europol.

### International conferences and workshops

#### The Computers, Privacy and Data Protection conference


The CPDP brings together academics, lawyers, practitioners, policy-makers, computer scientists and civil society to exchange ideas about data

protection and information technology. In January 2020, the EDPS organised a side event at the CPDP in which four invited speakers each presented and discussed their own innovative approaches on how to regulate or supervise AI. The EDPS also participated in several insightful and constructive panel discussions at the CPDP, with Supervisor Wojciech Wiewiórowski providing the [closing remarks](#) of the CPDP.

#### The Global Privacy Assembly

The GPA, previously known as the International Conference of Data Protection and Privacy Commissioners, continues to be the premier forum for more than 130 DPAs from across the globe to connect and share their perspectives on the developments in data protection and key elements of their international cooperation. The EDPS hosted the 2018 ICDPPC. In October 2020, the conference took place online for the first time due to the COVID-19 pandemic. During this conference, the


## Advancing Global Privacy in the Digital Age



**The European Data Protection Supervisor (EDPS)** is an active member of the **Global Privacy Assembly (GPA)**, which is formerly known as the International Conference of Data Protection and Privacy Commissioners (ICDPPC). The EDPS hosted the 2018 ICDPPC that gathered more than 1000 delegates discussing **Digital Ethics** and the challenges of a **Data Driven Society**.

For more than four decades, the Assembly has been the **premier global forum for data protection and privacy authorities**, providing leadership at international level and connecting the efforts of more than 130 supervisory authorities from across the globe. The Assembly supports Working Groups in the fields of international enforcement and cooperation, policy standards, consumer protection, digital economy and ethics, among others.

The Covid-19 pandemic worldwide means the annual conference in Mexico City is postponed until 2021. This year, instead, supervisory authorities will meet together online between 12-15 October to discuss key elements of their international cooperation. The EDPS promotes a fair and sustainable digital economy and a common vision on digitisation and technology. Our goal is to **shape a safer digital future** for all, as a building block of effective **international cooperation**.



A vibrant digital economy needs products and services that **respect the fundamental rights of individuals**. However, technological developments in the fields of Artificial Intelligence, machine learning and facial recognition puts the fundamental rights of the digital society at stake. Data can play a key role in health and well-being, the environment, transparent governance and other public services.

Data protection laws and regulations are necessary to ensure that data-driven business models benefit society as a whole and are sustainable in the long run. Policymakers and businesses who think long-term will realise that data protection and privacy regulations are indispensable for a digital society to be grounded in a trustworthy digital economy.

Data protection and privacy are the foundations for **democracy** in a time of digitisation. Technology should serve humankind and be re-engineered along the lines of **fundamental rights and values**, alongside **strict liability rules**.

[www.globalprivacyassembly.org/gpa2020/](http://www.globalprivacyassembly.org/gpa2020/)

EUROPEAN DATA PROTECTION SUPERVISOR

[www.edps.europa.eu](http://www.edps.europa.eu)

[@EU\\_EDPS](https://twitter.com/EU_EDPS)

[EDPS](https://www.linkedin.com/company/edps)

[European Data Protection Supervisor](https://www.youtube.com/user/EuropeanDataProtectionSupervisor)



EDPS continued to promote a fair and sustainable digital economy and a common vision on digitisation and technology. The Information and Communication team created an infographic to raise awareness of the GPA and our involvement in the GPA, to mark the occasion.

### **The 2020 Data Protection Workshop within International Organisations**

The EDPS initiated the Data Protection Workshop within International Organisations in 2005 to bring together international organisations to share their experience and best practice in the field of data protection, analyse its impact as part of good governance within international organisations and summarise regulatory developments at international level. In light of the COVID-19 pandemic, the [October 2020 workshop](#) was online, shorter and on the theme of “Data protection in international organisations in times of crisis”.

### **EDPS visual identity**

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

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

### **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 the EDPS and what we are doing, 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 the work of the EDPS.

We had 10 study visit requests in 2020, 2 of which we were able to host as in-person visits before the COVID-19 lockdown came into effect in March. Due to the national and EUI rules, we then had to refuse all in-person visits, but instead offered the option of an online presentation with a Q&A session. This was not practical for all the groups that requested a visit and we hosted one virtual study visit after the lockdown came into effect.

### **Information requests**

The number of public requests for information received by the EDPS increased in 2020. While we still receive many requests related to matters over which the EDPS has no competence (mainly because they are of national scope and not EU related), we have also received a growing number of requests in recent months which 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 information relevant to the individual 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.

## **5.2 Administration, budget and staff**

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

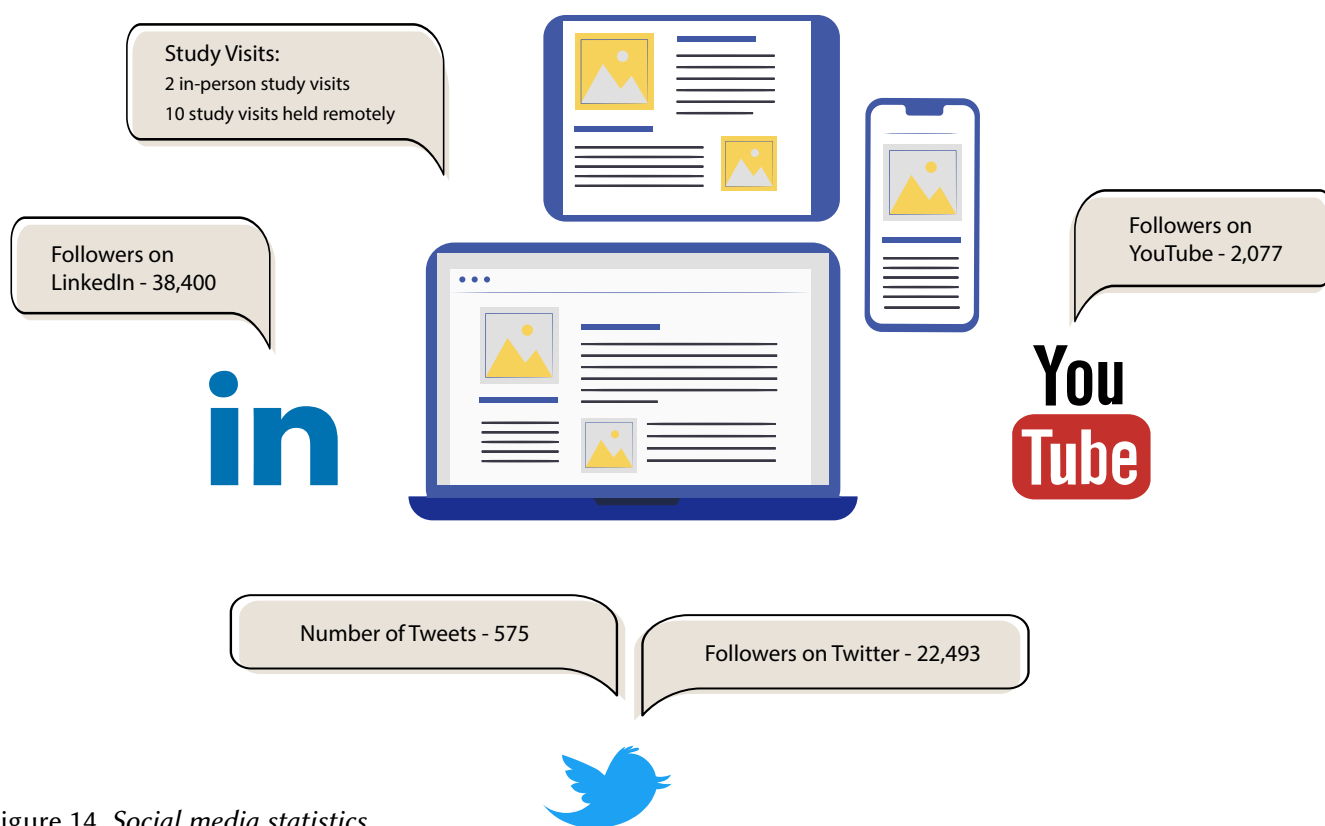


Figure 14. *Social media statistics*

HRBA has had to adapt its organisation in 2020 in light of the COVID-19 pandemic to ensure business continuity by developing an innovative action plan to enhance the functioning of the EDPS and the wellbeing of its staff, in particular preparing the workforce for teleworking.

### 5.2.1 Challenges during the COVID-19 pandemic

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

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

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

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

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

use disinfectant available in the building to ensure safe working conditions.

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

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

### 5.2.2 A growing organisation

The EDPS strives to bring together a diverse team of legal and technical experts, as well as other specialists in their field from all across the EU, working to shape the world of data protection and our organisation.

The EDPS continued to grow in 2020, both in terms of financial and human resources. The Budgetary Authority, pursuant to thorough HR forward planning, granted the EDPS the requested increase of staff that was deemed necessary to cope with the increased responsibilities assigned to the Institution.

Despite the exceptionally difficult context, HRBA kept recruiting as from the early stages of the first lockdown. This required agility, flexibility and creativity.

In 2019, a competition for specialists in data protection resulted in a reserve list of 33 laureates. The HRBA used this list to recruit new staff for the EDPS and the EDPB; now only one third of that list is remaining. The HRBA also recruited contract staff to fill in specific needs or positions temporarily free due to long absences.



### 5.2.3 Learning and development

In 2020, HRBA continued to offer general (including classroom and e-learning language courses), management (via the European School of Administration [EUSA]) and external training to EDPS staff. During work modalities 0 and 1, EDPS staff benefited from the European Commission's and EUSA's online training courses.

HRBA launched a 360 exercise in November 2020 to develop middle and senior managers' skills to boost staff's performance and ensure their well-being. There was an opportunity for EDPS staff to provide anonymous feedback to their respective managers on their needs regarding their professional development.

HRBA started *HRBA teasers* in 2019 and continued this initiative in 2020. These are short presentations covering procedures, tools and topics of interest for new colleagues. They aim to help newcomers to better understand the role and function of HRBA within the EDPS, which, in turn, improves everyday workplace proceedings. The teasers cover topics, such as internal IT systems and processes, a Q&A for newcomers and the EU learning and development platform.

HRBA has improved the welcoming of new colleagues. During work modalities 0 and 1, HRBA provided newcomers at the EDPS with information about and links to online training, as well as the opportunity to raise specific questions. HRBA published FAQ sections on the EDPS intranet to specifically target questions on procedures and work modalities during the COVID-19 pandemic.

Due to the pandemic, the welcoming of new colleagues who started their job at the EDPS remotely became even more important. Thus, HRBA resumed newcomers' welcome days during the first weeks following their arrival via a mandatory and reformatted virtual meeting of 2 short sessions during 2 consecutive days. Each key colleague gives a presentation to the newcomers and there is a collective exercise for newcomers to get to know each other and other key employees of the EDPS, such as the Director. The welcome days also provide reassurance that newcomers are well informed about the EDPS procedures.

### 5.2.4 Going paperless

Already commenced in 2019, the COVID-19 pandemic accelerated the process of the EDPS' efforts to becoming a paperless institution, now for reasons of business continuity and sanitation, as well as efficiency and the environment.

This process includes the continuation of paperless interviews in 2020, the intention to automate appraisal, probation and evaluation reports via the implementation of new modules in the human resources (HR) interface in 2021, and the implementation of the following finance systems in 2020:

- Speedwell, a system created by the European Research Council Executive Agency (ERCEA), for the processing of payments;
- Bluebell, a system created by the ERCEA, for budget management; and
- Case Management System (CMS), an internally developed system, for procurement.

The implementation of the Public Procurement Management Tool (PPMT) is still being considered.

### 5.2.5 Staff satisfaction survey and action plan

HRBA organise a satisfaction survey every two years in order to gauge an understanding of how EDPS staff view their overall working environment.

A report on the June 2020 survey, presented to EDPS staff in October 2020, demonstrated that the majority of EDPS staff are either satisfied or very satisfied with the nature and responsibilities of their job roles. However, as a follow-up to this survey, HRBA drafted a corresponding action plan, which was further accompanied by a discussion during an EDPS managers' remote away day in November 2020. HRBA has been able to use this action plan to improve the working environment at the EDPS in 2020 and will continue to do so in 2021.

### 5.2.6 New HRBA actions

HRBA has implemented a number of initiatives to improve the communication, collaboration and well-being of EDPS staff.

#### HRBA newsletter

In order to enhance the internal communication between HRBA, EDPS staff and EDPB colleagues, HRBA publishes a monthly newsletter containing useful information and reminders.

#### EDPB secondment programme

The [GDPR](#) entrusts the EDPB with the task of promoting the exchange of information, practices and common training programmes between DPAs. One way of doing this is through the temporary exchange of staff.

HRBA launched a pilot secondment programme in 2019 to facilitate this process, involving the exchange of staff members between DPAs themselves or between a DPA and the EDPB secretariat. However, the vast majority of these secondments had to be postponed due to the COVID-19 pandemic. Only one secondment could take place which, despite the lockdown, was a success both for the host (the Italian DPA) and for the hosted staff member of the EDPB. As soon as circumstances allow it, the foreseen secondment programmes will safely resume, as all stakeholders have expressed their interest in continuing this type of exchange.



### Job shadowing

The EDPS has decided to develop and implement a job-shadowing programme. While an informal type of job shadowing already existed at the EDPS, for example to ensure back up or the welcoming of new colleagues, it was deemed necessary to offer a formal framework and guidelines to EDPS staff.

Job shadowing promotes learning opportunities and the exchange of ideas between host and guest. This initiative will help EDPS staff to enhance their networking skills, explore opportunities, enhance or prepare mobility, giving or receiving feedback, and improve collaboration with different units and sectors across the EDPS and EDPB.

### EDPS well-being: a safe and positive working environment

The EDPS is a socially responsible organisation. One of our values is to treat people, including our staff, with respect. In order to build a positive, respectful and safe working environment, HRBA issued guidelines to recognise, prevent and manage staff burnout, and a review of the decision about the procedure relating to anti-harassment and the appointment of confidential counsellors.

The EDPS believes that staff with higher levels of well-being have been found to learn more effectively, be more creative, have better 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.

HRBA appointed a Well-being Coordinator to ensure that internal HR processes are in line with EDPS staff well-being, and that staff have the knowledge and tools necessary to facilitate a high level of well-being in (and whenever possible, outside) work. The Well-being Coordinator role is normally held by an HR representative, as a well-being-oriented approach immensely benefits recruitment and on-boarding, career planning, performance and succession management, engagement and recognition, off-boarding and retirement. The Well-being Coordinator applies the following principles

to every single interaction with current, former and future EDPS staff:

- encouraging an enjoyable working environment;
- giving staff a voice;
- making sure that the EDPS' values are demonstrated; and
- treating every person as a human being who matters.

### 5.2.7 Internal coaching and well-being

In 2020, HRBA continued to provide internal coaching to improve the individual job performance of EDPS and EDPB staff. 14 staff members took part in over 35 of these sessions in 2020. HRBA provided team coaching as well, for example a remote “away day” and SWOT exercise with the middle management led to an action plan focusing on team relations and setting priorities for 2020 and 2021 in the context of the COVID-19 pandemic.

During work modality 1, HRBA facilitated 7 voluntary “peer learning virtual chats” for EDPS staff to discuss their professional and personal experiences. HRBA shared the general outcomes of these sessions with management to address any general needs. HRBA set up a separate voluntary workshop on managing anxiety and stress caused by the COVID-19 pandemic.

HRBA also organised a voluntary and remote collective exercise for all EDPS staff to enhance their cohesion by identifying positive experiences during work modalities 0 and 1 that could be built upon in the future, encouraging a sense of belonging and cross team interactions, and enabling newcomers to meet colleagues. HRBA presented a report with the main outcomes of this exercise to management for follow up actions as appropriate. Up to 14 staff members attended each of these 8 sessions.

Inspired by an initiative in the European Commission, HRBA also organised 2 voluntary and random virtual coffee sessions for staff as a replacement for the ad hoc encounters that they



may usually have experienced in the EDPS building. Two pilot sessions were organised in December 2020.

## 5.2.8 Finance

The EDPS Finance Guide was updated in order to account for the main recommendations of the Court of Auditors and to render a more comprehensive guidance to all colleagues in the EUI involved, directly or indirectly, in financial management.

In order to increase the degree of business continuity for financial operations, the list of appointed financial actors was completed, accounting for the back-up arrangements of the different units and sectors. Another Authorising Officer by Sub delegation was appointed within the HRBA Unit to facilitate timely payment validation and payment contracting when management is prevented.

## 5.2.9 Procurement

HRBA prepared and published a “Procurement Process Guide” on the EDPS intranet in 2020, in order to provide EDPS staff with detailed guidance on different procurement procedures.

For planning purposes, the EDPS implemented for the first year a procurement plan, which was reviewed on a quarterly basis.

The EDPS implemented the EU electronic tender platforms eTendering and eSubmissions in its first open procedure of 2020. HRBA mostly carried out procedures that were very low value or implementing existing framework contracts, but also conducted procedures leading to the conclusion of new framework contracts such as the:

- supply of graphic design and printing services for the EDPS and the EDPB online and print publications, via a middle value negotiated procedure;
- production of video clips, via a middle value negotiated procedure; and
- annual report, via an open procedure.

The EDPS participates in interinstitutional framework contracts, such as the acquisition of IT software and IT and language training services, to improve efficiency.

## 5.2.10 Accounting

In 2020, a new accounting correspondent was appointed and trained on the relevant accounting and reporting software.

Although the accounting function is carried out by the Directorate-General for Budget (DG BUDG) under the Service Level Agreement (SLA) concluded with the EDPS, HRBA played a more active role assisting BUDG (execution of accounting controls, review of the closure methodology, etc.) in 2020.

## 5.2.11 Budget

The budgetary execution was substantially lower than last year due to COVID-19 related restrictions. These restrictions had, more particularly, an impact on the missions, travel costs and the organisation of and participation in events.

In the last quarter of 2020, the rollout of the new budget management tool, Bluebell, began. The main objectives for the implementation of this tool are to become more efficient during budget preparation and to improve the monitoring of budget implementation.

In order to allow a smooth transition to this new system, two pilot units (the EDPS’ Information and Communication Unit and the EDPB) worked directly in Bluebell. These units were trained and had their first hands-on experience.

With regard to the annual exercise of the establishment of the budget, it concerned not only the year 2021, but also the multiannual financial framework (MFF) for 2021-2027. The MFF sets annual maximum amounts (ceilings) for expenditure as a whole and for the main categories of expenditure. Consequently, this requires a thorough reflection, which was made even more difficult due to the COVID-19 pandemic and the potentially permanent



impact this could have on the way the Institution conducts its activities.

### 5.2.12 Administration

HRBA has maintained a fast pace to undertake administrative tasks as smoothly as possible, in accordance with the increasing needs and challenges of the EDPS.

In the context of the COVID-19 pandemic, HRBA tailored health and safety measures in 2020 by making masks and disinfectant available to staff, adapting meeting room occupancy and introducing signs for lifts, kitchenettes and sanitary rooms.

HRBA continued to build solid working relationships with other EUIs via administrative agreements, Memoranda of Understanding and Service Level Agreements, in order to ensure the effective and efficient running of the EDPS.

The EDPS started planning in 2020 to occupy the ground, second and seventh floor of the Montoyer 30 building, which the European Ombudsman is

foreseen to vacate in July 2021. Within the so-called House of Data Protection in the EU project, HRBA envisages to plan the necessary works, in cooperation with the European Parliament, for adequate office space to match current and future needs in terms of staff; and to transform some spaces into common areas such as enlarged meeting rooms with portable teleconferencing devices, a new Cloud (dedicated room for lunch time and coffee breaks) of our staff, an IT Lab, a press room, a library/study and a well-being room.



## THE DATA PROTECTION OFFICER (DPO) AT THE EDPS

The focus of the DPO office at the EDPS in 2020 was to continue the process of a smooth transition towards the data protection framework set out in [Regulation \(EU\) 2018/1725](#), while always keeping the role and mission of the EDPS in mind.

The EDPS is a small institution, tasked with responsibilities that influence the lives, dignity and fundamental rights of all individuals in the EU, as well as their relationships with other people, private entities and public administration.

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

Considering the EDPS' role as the data protection authority (DPA) of the EUIs as well as the high level of in-house expertise in the field, the DPO office, together with the services in charge of personal data processing, continued throughout 2020 to raise and uphold the highest standards of data protection to lead by example. 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'.

In line with its commitment, the EDPS appointed a full-time DPO in September 2020.

### 6.1 Accountability

The DPO office put accountability into practice in a number of ways in 2020.

After the adoption of a number of data protection internal rules and procedures (such as the [EDPS Decision](#) on DPO implementing rules and the [EDPS Decision](#) on Internal rules concerning restrictions of certain rights of data subjects), the DPO office, together with the responsible services, monitored the practical application of these rules and procedures.

Strengthening compliance has also been a significant focus of the work of the DPO office over the past year. This has involved:

- consolidating the [register of processing activities](#) with new and updated records;
- increasing transparency and accessibility for individuals by publishing new and updated data protection notices in the most appropriate sections of the internet and intranet, as well as improving clarity and comprehensiveness; and

## DATA PROTECTION OFFICER (DPO) AT THE EDPS

- beginning a process of scrutinising the services that the EDPS is using in order to clarify the EDPS' responsibilities, and those of the EUIs, as service providers, as well. This work will continue in 2021.

In addition, the DPO office has addressed requests made by the EDPS, as the data protection authority for EUIs. In particular, like other EUIs, following the order of the EDPS to map all transfers outside the European Union (EU) / European Economic Area (EEA) and its subsequent reporting obligation (as described in the EDPS [Strategy for EUIs to comply with “Schrems II” ruling](#)), the DPO office concluded its mapping exercise and submitted its report to the EDPS. After sending this report, the DPO office, together with the responsible services, has continued to closely monitor the situation and keep its mapping of international transfers updated in order to take the latest developments into account. The EDPS also started the process of exploring privacy and data protection friendly alternatives to limit reliance on services that involve transfers of personal data outside the EU and EEA.

### 6.2 Enquiries and complaints

The number of enquiries, complaints and requests from individuals exercising their data protection rights received by the EDPS in 2020 remained relatively stable in comparison with previous years.

Although there has been an increase in erasure requests, three of the four received in 2020 concerned situations where the EDPS was not processing the requesters' personal data. In the fourth case, after carrying out the verification, it was found that the personal data had been processed not long before the request, given that a similar request was done.

In 2020, the EDPS also received a complaint about the procedure regarding the identification of individuals exercising data protection rights. While the procedure was up-to-date and accounted for the data minimisation principle, the '[How to exercise your data protection rights at the EDPS](#)' section on the website needed to reflect also the practice and, as such, was updated.

In the context of the “[Schrems II](#)” ruling, a request for information was submitted to the EDPS inquiring whether the requester's personal data was transferred outside of the EU and particularly to the US. Following verification, the requester was informed that a transfer of personal data outside the EU took place. The EDPS continues to follow-up on the matter and scrutinises transfers outside of the EU and EEA, including the legal instruments employed for transfers. Another request for information concerned the cookies banner of the EDPS website; this was clarified after the requester looked into browsers' settings.

The EDPS continued throughout the year to work towards increasing its compliance, as well as towards streamlining its procedures on handling requests of individuals exercising their data protection rights.

### 6.3 Advising the EDPS

The DPO office continued throughout 2020 to advise services in charge of personal data processing on a wide variety of subject matters.

In particular, the DPO office advised on data protection compliance of services considered to be used by the EDPS, in the fields of human resources, information security and cloud services. In many cases, a number of safeguards were put in place to ensure compliance, including specific contractual terms tailored to the relevant circumstances. Considering the central topic of the year, the DPO office also advised and worked closely with services in charge of COVID-19-related personal data processing.

In addition, the DPO office was regularly consulted on the legal provisions of new and updated Service Level Agreements (signed chiefly with the European Commission and the European Parliament as providers of essential services for the EDPS), Memoranda of Understanding and the review of certain internal rules and procedure (such as appraisal and anti-harassment).

### 6.4 Awareness-raising

The DPO office delivered a number of training sessions in 2020.

All new colleagues' training sessions incorporate a module on data protection, which is regularly updated to take into account the latest developments in the field, including the most recent internal EDPS 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 than general data protection concepts.

There were also specific information sessions and training. To raise awareness on personal data breaches, a specific information session on the topic was organised focusing on theoretical aspects as well as the examination of specific situations. This specific training aimed to both inform EDPS staff about the topic and, equally, to reduce these kind of occurrences and mitigate their risks.

a particular social media platform by DPAs, with a specific emphasis on controllership, legal bases and categories of personal data processed.

### 6.5 Collaboration with DPOs of other EUIs

The DPO office continued its collaboration with the correspondent offices of other EUIs, allowing for the valuable exchange of expertise and best practice, in various fora (such as regular and ad-hoc meetings, and working groups on specific topics) gathering DPOs and other experts.

The DPO office participated in the biannual meetings with the DPOs of the other EUIs and with the EDPS (in May 2020 and December 2020). Various topical subject matters were discussed, amongst which challenges of processing personal data in times of pandemic, the use of social media and its challenges, international transfers, as well as fostering cooperation between the EUIs' DPOs and the EDPS.

The DPO office also participated in the regular meetings organised by the DPOs' network of the EDPB, comprised of DPOs of national DPAs. The focus of its work in 2020 was on assessing the use of

# 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.



# 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);

- a. 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.
2. The European Data Protection Supervisor shall have the following corrective powers:
    - a. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
    - b. to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
    - c. to refer matters to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;
    - d. 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;
    - e. 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;

## 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. to impose a temporary or definitive limitation including a ban on processing;
  - g. 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;
  - h. 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;
  - i. to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.



3. The European Data Protection Supervisor shall have the following authorisation and advisory powers:
  - a. to advise data subjects in the exercise of their rights;
  - b. to advise the controller in accordance with the prior consultation procedure referred to in Article 40, and in accordance with Article 41(2);
  - c. 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;
  - d. to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 48(2);
  - e. to authorise contractual clauses referred to in point (a) of Article 48(3);
  - f. to authorise administrative arrangements referred to in point (b) of Article 48(3);
  - g. to authorise processing operations pursuant to implementing acts adopted under Article 40(4).
4. 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.
5. 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.

## LIST OF DATA PROTECTION OFFICERS IN 2020

<b>Council of the European Union</b>	Reyes OTERO ZAPATA
<b>European Parliament</b>	Secondo SABBIONI
<b>European Commission</b>	Martin KRÖGER Niels Bertil RASMUSSEN
<b>Court of Justice of the European Union</b>	Joris PLINGERS Ivana BOŽAC
<b>Court of Auditors</b>	Johan VAN DAMME
<b>European Economic and Social Committee (EESC)</b>	Lucas CAMARENA Simone BAPTISTA
<b>Committee of the Regions (CoR)</b>	Antonio FIGUEIRA
<b>European Investment Bank (EIB)</b>	Pelopidas DONOS Laurence WAERENBURGH Anca Popa
<b>European External Action Service (EEAS)</b>	Emese SAVOIA-KELETI
<b>European Ombudsman</b>	Francesca PAVESI Nicholas HERNANZ
<b>European Data Protection Board (EDPB)</b>	Joao SILVA Nerea PERIS BRINES Panagiota KALYVA

<b>European Data Protection Supervisor (EDPS)</b>	Constantin CHIRA PASCANUT Marco MORESCHINI
<b>European Central Bank (ECB)</b>	Maarten DAMAN
<b>European Anti-Fraud Office (OLAF)</b>	Veselina TZANKOVA Christina KARAKOSTA
<b>Translation Centre for the Bodies of the European Union (CdT)</b>	Martin GARNIER
<b>European Union Intellectual Property Office (EUIPO)</b>	Gloria FOLGUERA VENTURA
<b>Agency for Fundamental Rights (FRA)</b>	Robert Jan Uhl Abigail Clayton
<b>Agency for the Cooperation of Energy Regulators (ACER)</b>	Marina ZUBAC Stefano VAONA
<b>European Medicines Agency (EMA)</b>	Stefano MARINO Orsolya EÖTVÖS
<b>Community Plant Variety Office (CPVO)</b>	Gloria FOLGUERA VENTURA
<b>European Training Foundation (ETF)</b>	Tiziana CICCARONE Laurens RIJKEN
<b>European Asylum Support Office (EASO)</b>	Alexandru George GRIGORE
<b>European Network and Information Security Agency (ENISA)</b>	Athena BOURKA Ingrida TAURINA
<b>European Foundation for the Improvement of Living and Working Conditions (Eurofound)</b>	Mafalda AGUIAR
<b>European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)</b>	Ignacio VÁZQUEZ MOLINÍ
<b>European Food Safety Authority (EFSA)</b>	Claus REUNIS
<b>European Maritime Safety Agency (EMSA)</b>	Radostina NEDEVA MAEGERLEIN, Oana Roxana IUGAN
<b>European Centre for the Development of Vocational Training (CEDEFOP)</b>	Jesús BUSTAMANTE
<b>Education, Audiovisual and Culture Executive Agency (EACEA)</b>	Nicolas DURAND Anber EVANS

## ANNEXES

<b>European Agency for Safety and Health at Work (EU-OSHA)</b>	Michaela SEIFERT
<b>European Fisheries Control Agency (EFCA)</b>	Stefano DONADELLO Marta RAMILA HIDALGO
<b>European Union Satellite Centre (SATCEN)</b>	Joana GONÇALVES Maria CHATZIANGELIDOU
<b>European Institute for Gender Equality (EIGE)</b>	Ieva VASILIONE Nicasio LOPEZ RODRIGUEZ
<b>European GNSS Agency (GSA)</b>	Ezio VILLA Nikitas NIKITARAS
<b>European Union Agency for Railways (ERA)</b>	Zografia PYLORIDOU
<b>Consumers, Health and Food Executive Agency (Chafea)</b>	Yolanda AREVALO TORRES Alina PYDA
<b>European Centre for Disease Prevention and Control (ECDC)</b>	Andrea IBER
<b>European Environment Agency (EEA)</b>	Olivier CORNU Helle MOLLER Eleni Barla
<b>European Investment Fund (EIF)</b>	Paolo SINIBALDI
<b>European Border and Coast Guard Agency (Frontex)</b>	Nayra PEREZ Julia ANTONOVA
<b>European Securities and Markets Authority (ESMA)</b>	Sophie VUARLOT-DIGNAC
<b>European Aviation Safety Agency (EASA)</b>	Carla RAMOS Elena TELLADO VÁZQUEZ
<b>Executive Agency for Small and Medium-sized Enterprises (EASME)</b>	Elke RIVIERE Anthony BISCH
<b>Innovation and Networks Executive Agency (INEA)</b>	Caroline MAION Venetia PAPASYMEON Athina KOSMA
<b>European Banking Authority (EBA)</b>	Jonathan OVERETT SOMNIER
<b>European Chemicals Agency (ECHA)</b>	Bo BALDUYCK
<b>European Research Council Executive Agency (ERCEA)</b>	Roberta MAGGIO



<b>Research Executive Agency (REA)</b>	Maria Francisca BRUNET-COMPANY Sergejs TROFIMOV
<b>European Systemic Risk Board (ESRB)</b>	Maarten DAMAN
<b>Fusion for Energy</b>	Walter SCHUSTER Raymond MONK
<b>SESAR Joint Undertaking</b>	Laura GOMEZ GUTIERREZ Vicenca DA SILVA
<b>ECSEL</b>	Anne SALAÜN
<b>Clean Sky Joint Undertaking</b>	Bruno MASTANTUONO
<b>Innovative Medicines Initiative Joint Undertaking (IMI)</b>	Sebastien PECHBERTY Desmond BARRY
<b>Fuel Cells &amp; Hydrogen Joint Undertaking</b>	Georgiana BUZNOSU
<b>European Insurance and Occupations Pensions Authority (EIOPA)</b>	Catherine COUCKE
<b>European Agency for Law Enforcement Training (CEPOL)</b>	Ioanna PLIOTA
<b>European Institute of Innovation and Technology (EIT)</b>	Nora TOSICS
<b>European Defence Agency (EDA)</b>	Clarisse RIBEIRO
<b>Body of European Regulators for Electronic Communications (BEREC)</b>	Marco DE SANTIS
<b>European Union Institute for Security Studies (EUISS)</b>	Nikolaos CHATZIMICHALAKIS
<b>eu-LISA</b>	Encarna GIMENEZ
<b>Bio-Based Industries Joint Undertaking</b>	Marta CAMPOS-ITURRALDE
<b>Europol</b>	Daniel DREWER
<b>EFTA Surveillance Authority (ESA)</b>	Kjersti SNEVE
<b>Shift2Rail Joint Undertaking</b>	Isaac GONZALEZ GARCIA

<b>Single Resolution Board (SRB)</b>	Esther BRISBOIS
<b>EUROJUST</b>	Diana ALONSO BLAS





# LIST OF OPINIONS AND FORMAL COMMENTS ON LEGISLATIVE PROPOSALS

## Opinions

Please refer to the [EDPS website](#) for translations and executive summaries.

In 2020, the EDPS issued Opinions on the following subjects (date of issuance in brackets):

- Preliminary Opinion on data protection and scientific research ([6 January 2020](#))
- Opinion on the International agreement on exchange of personal data between Europol and New Zealand ([31 January 2020](#))
- Opinion on the opening of negotiations for a new partnership with the UK ([24 February 2020](#))
- Opinion on the European Strategy for Data ([16 June 2020](#))
- Opinion on the European Commission's White Paper on Artificial Intelligence - A European approach to excellence and trust ([29 June 2020](#))
- Opinion on the European Commission's action plan for a Comprehensive Union policy on preventing money laundering and terrorism financing ([23 July 2020](#))
- Opinion on the proposal for an amendment of Council Directive 2011/16/EU relating to administrative cooperation in the field of taxation ([28 October 2020](#))
- Opinion on the proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online ([10 November 2020](#))
- Preliminary Opinion on the European Health Data Space ([17 November 2020](#))
- Opinion on the New Pact on Migration and Asylum ([30 November 2020](#))
- Opinion on the opening of negotiations on Eurojust cooperation with competent authorities of certain 3rd countries (16 December 2020)

## Formal Comments

Please refer to the [EDPS website](#) for translations of the Formal Comments in French and German.

In 2020, the EDPS issued Formal Comments on the following subjects (date of issuance in brackets):

- Formal Comments on the model status agreement concluded by the EU with third countries (29 May 2020)
- Formal Comments on the proposal for a Council Directive amending Directive 2011/16/EU due to the COVID-19 pandemic ([12 June 2020](#))

- Formal Comments on a draft Commission Implementing Regulation amending Implementing Regulation (EU) No 1352/2013 ([24 June 2020](#))
- Formal Comments on the model working arrangements between the European ad Coast Guard Agency and the authorities of third countries ([3 July 2020](#))
- Formal Comments on cross-border exchange of data between COVID-19 contact tracing and warning mobile applications ([9 July 2020](#))
- Formal Comments on the draft Delegated Regulation amending Delegated Regulation 2015/2446 and Delegated Regulation (EU) 2016/341 ([17 July 2020](#))
- Formal Comments on the draft Commission Delegated Regulation amending Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office as regards setting out categories of operational personal data and categories of data subjects for the purpose of data processing in the index ([31 July 2020](#))
- Formal Comments on establishing technical specifications and procedures required for the system of interconnection ([31 July 2020](#))
- Formal Comments on draft Commission Implementing Decision on the technical rules necessary for entering, updating, deleting and searching data in the Schengen Information System and other implementing measures ([26 August 2020](#))
- Formal Comments on the draft Commission Implementing Decisions on the minimum standards and technicalities for biometric data in the Schengen Information System in the field of border checks and return and the field of police and judicial cooperation ([26 August 2020](#))
- Formal comments on the draft Commission Delegated Regulation supplementing Directive (EU) 2010/31 of the European Parliament and of the Council ([28 August 2020](#))
- Formal Comments on draft Implementing Regulation amending Implementing Regulation 2015/2447 ([28 August 2020](#))
- EDPS Formal comments on the draft Commission Implementing Decision on the keeping and accessing of the logs in the European Travel Information and Authorisation System (ETIAS) pursuant to point (b) of the third subparagraph of Article 73(3) of Regulation (EU) 2018/1240 of the European Parliament and the Council (04 September 2020)
- EDPS Formal comments on the draft Commission Implementing Decision laying down performance requirements of the European Travel Information and Authorisation System (ETIAS) pursuant to point (b) of the third subparagraph of Article 73(3) of Regulation (EU) 2018/1240 of the European Parliament and the Council (04 September 2020)
- EDPS Formal comments on the draft Commission Implementing Decision on the rules on the operation of the public website and the app for mobile devices, pursuant to Article 16(10) of Regulation (EU) 2018/1240 of the European Parliament and of the Council (04 September 2020)
- EDPS Formal comments on the draft Commission Implementing Regulation on reporting of abuses pursuant to Article 15(5) of Regulation (EU) 2018/1240 (04 September 2020)
- EDPS Formal comments on the draft Commission Delegated Decision laying down the measures for flagging pursuant to Articles 36(4) and 39(2) of Regulation (EU) 2018/1240 of the European Parliament and of the Council (04 September 2020)
- EDPS Formal comments on the draft Commission Delegated Regulation laying down the predetermined list of job groups used in the application form, pursuant to Article 17(3) of Regulation (EU) 2018/1240 of the European Parliament and of the Council (04 September 2020)

- Formal Comments of Implementing Decision on the specifications and conditions for the website, pursuant to Article 50(5) of Regulation (EU) 2017/2226 of the European Parliament and of the Council (01 October 2020)
- Formal comments on the Proposal for a Council Decision on the position to be taken on behalf of the European Union in the EU-Canada Joint Customs Cooperation Committee as regards the adoption of the decision concerning the mutual recognition of the Partners in Protection Programme of Canada and the Authorised Economic Operators Programme of the European Union (20 November 2020)
- Formal Comments on the draft Commission Implementing Decision amending the Annex to Commission Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) ([20 November 2020](#))
- Formal Comments on a Proposal for a Regulation of the European Parliament and of the Council establishing the European Union Single Window Environment for Customs and amending Regulation (EU) No 952/2013 (20 November 2020)
- Formal Comments on the Implementing Decision Implementing Decision laying down requirements concerning the format of personal data to be inserted in the application form to be submitted pursuant to Article 17(1) of Regulation (EU) 2018/1240 of the European Parliament and the Council as well as the parameters and the verifications to be implemented in order to ensure completeness of the application and coherence of those data (07 December 2020)
- Formal Comments on the Implementing Regulation on technical arrangements for developing, maintaining and employing electronic systems for the exchange of information and for the storage of such information under the Code (11 December 2020)
- Formal Comments on the ETIAS- Implementing Decision on defining requirements concerning the format of personal data to be inserted in the application form to ensure competence and coherence (17 December 2020)



# LIST OF CONSULTATIONS AND PRIOR CONSULTATIONS ISSUED IN 2020

## Consultations

Please refer to the [EDPS website](#) for translations of the consultations in French and German.

In 2020, the EDPS issued 68 Consultations (26 informal opinions at staff level, 42 formal opinions) under Regulation (EU) 2018/1725 and the specific Regulations on Europol, Eurojust and EPPO.

The main topics dealt with include restrictions to data subjects' rights (13), data transmission and transfer (11), internal rules on data protection including on the DPO (10), controller-processor relationship (4), Covid-related issues (4) the right of access (4) and modifications of Europol's Opening Decisions of Analysis Projects (3).

The consultations mentioned in this report relate to the following subjects (date of publication in brackets):

- Legal basis for personal data transfers to the European University Institute in Florence ([12 November 2020](#))
- Notion of 'large scale' processing Article 39(3) (b) of Regulation (EU) 2018/1725 ([31 August 2020](#))
- B-Management of broad access requests ([23 July 2020](#))

- Nature of the relationship between an EUI and its travel agency ([3 June 2020](#))
- Arrangement involving transfers of personal data from an EUI to an international organisation ([3 June 2020](#))
- Agreement for payroll services for local employees in a third country ([6 May 2020](#))
- Use of telecommunication data to monitor spread of COVID-19 ([25 March 2020](#))
- Powers of the Authority for European Political Parties and European Political Foundations (APPF) and data protection obligations ([26 February 2020](#))
- Access to a staff member's complaint by Management Board Members of an EUI ([20 February 2020](#))
- Access to Passenger Name Record ('PNR') information

Other consultations are available on the EDPS website: Consultations on Administrative Measures and [Consultations on data protection matters](#)



## Prior Consultations

Please refer to the [EDPS website](#) for translations of the consultations in French and German.

In 2020, the EDPS issued Opinions following prior Consultation on the following subject (date of publication in brackets):

- Opinion on the European Public Prosecutor's Office's prior consultation on the risks identified in the Data Protection Impact Assessment carried out on its Case Management System ([1 October 2020](#))
- Opinion on a cryptocurrency webportal for law enforcement to query open source blockchain ([see also EDPS Annual report of 2019](#))
- Opinion on Europol's Online Service Provider Referral System
- Opinion on the implementation of the new Schengen Information System (SIS II) legal framework at Europol

# **SPEECHES BY THE SUPERVISOR WOJCIECH WIEWIÓROWSKI IN 2020**

## **European Parliament**

Wojciech Wiewiórowski, concluding remarks before the Civil Liberties, Justice and Home Affairs (LIBE) Committee at the hearing on *Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, European Parliament, Brussels, Belgium (20 February 2020).

Wojciech Wiewiórowski, “Annual Report 2019”, presented at the LIBE committee (Brussels, 18 March 2020).

Wojciech Wiewiórowski, “The use of personal data in the fight against Covid-19”, speech at the LIBE committee (Brussels, 7 May 2020, video link).

Wojciech Wiewiórowski, speech at the 7th Joint Parliamentary Scrutiny Group on Europol (via video link), Brussels, Belgium (28 September 2020).

## **Council of the European Union**

Wojciech Wiewiórowski, Presentation of the 2021 EDPS-EDPB budget at the Budget Committee, Brussels, Belgium (29 June 2020).

## **International Conferences**

Wojciech Wiewiórowski, *New Technologies and Old Questions. Challenges of Personal Data Protection in 2020*, speech at the Croatian Presidency Conference Data Protection Day 2020: Facing new challenges, Zagreb, Croatia (16 January 2020).

Wojciech Wiewiórowski, *World Café on enforcement of data protection in AI systems*, speech at the EDPS side event of the international conference *Computers, Privacy and Data Protection (CPDP) 2020*, Brussels, Belgium (21 January 2020).

Wojciech Wiewiórowski, speech at the EDPS-IPEN panel on web tracking, a side event of the international conference *Computers, Privacy and Data Protection (CPDP) 2020*, Brussels, Belgium (21 January 2020).

Wojciech Wiewiórowski, speech at the EDPS-Civil Society *Summit, Privacy Camp 2020*, Brussels, Belgium (21 January 2020).

Wojciech Wiewiórowski, *Data Protection AD 2020 and Beyond* closing keynote speech at the CPDP, (Brussels, 24 January 2020).

Wojciech Wiewiórowski, ‘Privacy and the Pandemic: The Role of Data Protection and Data Processing in Fighting COVID-19’, keynote speech at the Institute of International and European Affairs (IIEA) (via

video link), Dublin, Ireland (9 September 2020).

Wojciech Wiewiórowski, *“Doing the Utmost to Assist All Union Institutions: Reflections from the new European Data Protection Wojciech Wiewiórowski”* speech at the conference *“Nordic Privacy Arena 2020: The Brave New World – a human touch to a human right requires data privacy as a key ingredient”* (Stockholm, 5 October 2020) video link.

Wojciech Wiewiórowski, *“State of biometrics - GDPR Perspective”*, keynote speech delivered at *“the Biometrics Institute Congress 2020”* organised by the Biometrics Institute (Brussels, 7 October 2020), video link.

Wojciech Wiewiórowski, opening speech, Online Workshop: Data Protection within International Organisations 2020, Brussels, Belgium (8 - 9 October 2020).

Wojciech Wiewiórowski, *“New technologies and humanitarian action”* speech at the 21st edition of Bruges Colloquium on International Humanitarian Law. *“New Technologies on the Battlefield: Friend or Foe”* in the session entitled *“Data protection provisions framing the digital identity and biometrics (and the main problematic areas)”* organized by the International Committee of the Red Cross and the College of Europe in Bruges (Brussels, 12-16 October 2020), video link.

Wojciech Wiewiórowski, participation at the Global Privacy Assembly 2020 (GPA) (via video link), Brussels, Belgium (13 October - 15 October 2020).

Wojciech Wiewiórowski, speech at the Annual Privacy Forum 2020 (via video link), Brussels, Belgium (22 October 2020).

Wojciech Wiewiórowski, *“Bringing Research & Policy Together”*, speech at the international conference of the European Network Security Agency ENISA *“Annual Privacy Forum 2020”* organized jointly by Enisa, DG CONNECT and the Católica University of Portugal, Lisbon school of Law (Brussels, 22 October 2020), video link.

Wojciech Wiewiórowski, *“Current Development in EU Law”*, closing keynote speech at the conference *“Freedom Not Fear 2020”*, organized by the FreedomNotFear association, (Brussels, 7 November 2020), video link.

Wojciech Wiewiórowski, *High-level dialogue for a globalised world*, speech at event organised by the American European Community Association (AECA) (via video link), Brussels, Belgium (9 November 2020).

Wojciech Wiewiórowski, *“Real world data - a key to trustworthy artificial intelligence made in Europe?”*, speech at the High-Level Conference *“Digital Health 2020 – EU on the Move”*, organised by the German Federal Ministry of Health as part of the German Presidency in the Council of the European Union, (Brussels, 11 November 2020), video link.

Wojciech Wiewiórowski, *“GDPR assessment - an EU perspective”*, keynote speech at the 6th Annual Conference on Personal Data Protection *“The GDPR review after two years since entry into force”* - speech (Warsaw, 23 November 2020), video link.

Wojciech Wiewiórowski, *“International data transfers after the European Court’s Schrems II judgment”*, speech at the 33rd Annual International Conference Privacy Law & Business conference *“Nowhere to Hide”* (London, 26 November 2020), video link.

Wojciech Wiewiórowski, 4th Annual Brussels Privacy Symposium 2020 entitled *“Research and the Protection of Personal Data under the GDPR”*, closing keynote speech at the conference organised by the Future of Privacy Foundation and Vrije Universiteit Brussel (Brussels, 2 December 2020), video link.

Wojciech Wiewiórowski, *“Data protection landscape during uncertain times”*, keynote speech at the conference *“PrivSec Global 2020”*, organised by PrivacySeC Global, (2 December 2020), video link.

Wojciech Wiewiórowski, *“5G and the Protection of Persona Data”*, speech at the International Conference *“5G Italy - and the Recovery Fund”* organized by the by the Italian National Inter-University Consortium for Telecommunications (CNIT), (Rome, 3 December 2020) video link.

Wojciech Wiewiórowski, “*On the importance of collective wisdom of DPOs*” keynote speech at the Annual Conference organised by DPO Circle, (Brussels, 4 December 2020), video link.

Wojciech Wiewiórowski, “*The 10th Annual European Data Protection and Privacy Conference*”, keynote speech, organised by the Forum of Europe (Brussels, 8 December 2020), video link.

Wojciech Wiewiórowski, “*Shaping a Safer Digital Future: A New Strategy for a New Decade*”, presentation, part of the series, “*High level dialogue for a globalised world*”, organized by the American European Community Association (AECA) (Brussels, 9 December 2020), video link.

Wojciech Wiewiórowski, “*Cybersecurity Competence Centre Network pilots CONVERGENCE*” speech at the conference “*Making The European Cybersecurity Competence Network A Reality*” a joint event of the four Horizon 2020 projects Cybersec4Europe, SPARTA, CONCORDIA and ECHO (Brussels, 9 December 2020), video link.

Wojciech Wiewiórowski, “*Moving away from freedom v. Security tune*” speech at the conference “*EDEN goes to the Island – 5th EDEN Event on Data Protection in Law Enforcement*”, organised by the Academy of European Law (ERA) in cooperation with Europol’s Data Protection Experts Network (EDEN), (The Netherlands, 17 December 2020), video link.

## Other EU institutions and bodies

Wojciech Wiewiórowski, speech at the College of Eurojust, The Hague, Netherlands (11 February 2020).

Wojciech Wiewiórowski, speech at the European Medicine Agency (EMA) (via video link), Brussels, Belgium (4 May 2020).

Wojciech Wiewiórowski, speech at the 7th Joint Parliamentary Scrutiny Group on Europol (via video link), Brussels, Belgium (28 September 2020).

Wojciech Wiewiórowski, welcome address at *Global warming: Law Enforcement in the Age of Big Data, AI, Democracy Under Threat*, event organised by the Europol Data Protection Experts Network (EDEN) (via video link), Brussels, Belgium (15 October 2020).

## Other events

Wojciech Wiewiórowski, *Human Datafication as a way to the world of ‘inhuman’ rules*, speech at the “*Digital twin*” conference organized by the Office for Personal Data Protection and the Chair of Constitutional Law at the Faculty of Law, Administration and Economics of the University of Wrocław, (Wrocław, 10 January 2020).

Wojciech Wiewiórowski, opening speech at the EDPS-EDPB conference *The Circle of e-Life - a Lifetime Relationship with your Data*, Brussels, Belgium (27 January 2020).

Wojciech Wiewiórowski, *Facial recognition as a challenge for data protection law*, guest lecture at the University of Leiden, The Hague, Netherlands (11 February 2020).

Wojciech Wiewiórowski, opening remarks at the *EDPS Workshop on Artificial Intelligence and Facial Recognition: the EU Approach*, Brussels, Belgium (13 February 2020).

Wojciech Wiewiórowski, speech at the *CyberSec4Europe Panel Discussion on the European Cybersecurity Competence Network and Centre*, (via video link), Brussels, Belgium (24 February 2020).

Wojciech Wiewiórowski, “*EU Digital Solidarity: a call for a pan-European approach against the pandemic*” video message on the EDPS response to COVID-19 outbreak (6 April 2020), video.

Wojciech Wiewiórowski, introductory remarks before the Committee for European Affairs of the French Senate (via video link), Paris, France (27 April 2020).

Wojciech Wiewiórowski, *Data Protection at the Time of Plague. The European Union Approach*, lecture (via

video link) at the University of Warsaw, Poland (30 April 2020).

Wojciech Wiewiórowski, *EU and member states answer Covid-19 crisis with mobile apps. Privacy and data protection perspective*, lecture (via video link) at the University of KU Leuven, Brussels, Belgium (4 May 2020).

Wojciech Wiewiórowski, speech at the meeting (via video link) of Data Protection Officers of the EU institutions (8 May 2020).

Wojciech Wiewiórowski, keynote speech at a webinar organised by Slovak civil societies about human rights implications of contact tracing apps, (via video link), (15 May 2020).

Wojciech Wiewiórowski, keynote speech at the virtual IPEN Workshop on State of the art in encryption & its role as a safeguard for data protection and privacy, (via video link), Brussels, Belgium (3 June 2020).

Wojciech Wiewiórowski, *EDPS: Current priorities and challenges*, speech at the Summer Academy for Global Privacy Law 2020 (via video link), Brussels, Belgium (24 June 2020).

Wojciech Wiewiórowski, *the EU data protection system faced with artificial intelligence and machine learning – the future legal framework for Artificial Intelligence (AI)*, speech at the Annual Conference on EU Data Protection Law 2020 (via video link), Brussels, Belgium (25 June 2020).

Wojciech Wiewiórowski, *“Projecting privacy and data protection in a responsible, sustainable future”* presentation of the 2020-2024 EDPS Strategy (via video link), Brussels, Belgium (30 June 2020).

Wojciech Wiewiórowski, opening speech at the second meeting of the Hague Forum in cooperation with the Dutch Ministry of Justice and Security (Strategic Vendor Management Microsoft) and the European Commission (via video link), Brussels, Belgium (2 July 2020).

Wojciech Wiewiórowski, opening speech at the

data protection in the age of COVID-19. *Yesterday - Today - Tomorrow*, webinar organised by the EDPS and EDPB trainees, Brussels Belgium (7 July 2020).

Wojciech Wiewiórowski, *“AI in judicial systems - data protection perspective”*, Speech at the conference *“Access to Justice in the Digital Age”*, organised by German Presidency of the EU Council - (16-17 July 2020), video link.

Wojciech Wiewiórowski, *“Privacy and The Pandemic: The Role of Data Protection and Data Processing in Fighting Covid-19”*, keynote speech at the conference organised by the Institute of International and European Affairs (IIEA), (9 September 2020), video link.

Wojciech Wiewiórowski, speech at *think. BDPST 2020 – Connect to the future - Innovative Regulation, Regulatory Innovation* (via video link), Brussels, Belgium (2 October 2020).

Wojciech Wiewiórowski, speech at the Nordic Privacy Arena (via video link), Brussels, Belgium (5 October 2020).

Wojciech Wiewiórowski, *“Contact Tracing Apps”*, keynote speech at the conference *“IPEN 2020 Contact Tracing Apps”*, organised by EDPS (21 October 2020), video link.

Wojciech Wiewiórowski, *The Schrems II Mandate: Do what you can't?* Speech at the Centre for Information Policy Leadership (CIPL) Virtual Roundtable, (via video link) Brussels, Belgium (21 October 2020).

Wojciech Wiewiórowski, speech at the ITU Virtual Digital World 2020, (via video link) Brussels, Belgium (22 October 2020).

Wojciech Wiewiórowski, *“Hitch-hiker’s Guide to Cybersecurity AD 2020: Journal of the Year of Plague”* speech during the 12th Conference *“Internet Security”* entitled *“Cyberpandemic”*, Cardinal Stefan Wyszyński University (Warsaw, 22 October 2020), video link.

Wojciech Wiewiórowski, *“Schrems II, Privacy Shield*

*and Data Transfers – perspective of the European data protection authority*”, speech at the “EELA Virtual Seminar”, organised by the European Employment Lawyers Association (Brussels 28 October 2020), video link.

Wojciech Wiewiórowski, *Status of administrator in public sector conference. Case study: Division of roles and contractual safeguards between EU institutions and Microsoft, presentation at the Status of administrator in public sector’ conference organised by the University of Łódź (via video link), Brussels, Belgium (5 November 2020).*

Wojciech Wiewiórowski, *The EU technological and digital sovereignty: the hard role of mediation with OTT and the relations with the US*, speech at the Security Summit organised by CLUSIT (via video link), Brussels, Belgium (12 November 2020).

Wojciech Wiewiórowski, *“The Future of Encryption in the EU”*, keynote speech at the conference “ISOC 2020” organised by the Internet Society (19 November 2020), video link.

Wojciech Wiewiórowski, *“Hitch-hiker’s Guide to Personal Data Protection AD 2020: Journal of the Year of Plague”*, lecture at Leiden University, organised by the Center for Law and Digital Technologies (eLaw), (The Netherlands, 4 December 2020), video link.

Wojciech Wiewiórowski, *“From ‘precogs’ to ‘predictive justice’. Artificial intelligence used by the Police and judicial authorities in criminal matters”*, Lecture at KU Leuven University (via video link), Brussels, Belgium (8 December 2020).

Wojciech Wiewiórowski, *speech at the 10th Annual European Data Protection and Privacy Conference Responsible Data Use in Data-Driven Societies* (via video link), Brussels, Belgium (8 December 2020).





## THE EDPS

### Supervisor

Wojciech WIEWIÓROWSKI

### Director

Leonardo CERVERA NAVAS  
*Director*

Sylvie PICARD  
*Internal Control Coordinator*

Maria José SALAS MORENO  
*Administrative Assistant*

Achim KLABUNDE  
*Advisor to the Supervisor*

Constantin CHIRA-PASCANUT  
*DPO*

Tsanko TSANKOV  
*Transparency Officer*

### Cabinet of the Supervisor

Christian D'CUNHA\*  
*Head of Private Office*

Anna COLAPS  
*Member of the Cabinet*

Kazimierz UJAZDOWSKI  
*Member of the Cabinet*

Maria José SALAS MORENO  
*Personal Assistant to the Supervisor*

### Supervision and Enforcement

Delphine HAROU  
*Head of Unit*

Claire GAYREL  
*Deputy Head of Unit*

Petra CANDELIER  
*Head of Complaints and Litigation*

Owe LANGFELDT\*  
*Head of Consultations*

Ute KALLENBERGER  
*Head of Audits*

Bénédicte RAEVENS  
*Head of Consultations*

Stephen ANDREWS  
*Supervision and Enforcement Assistant*

Periklis TSELLOS  
*Supervision and Enforcement Assistant*

Guillaume BYK  
*Legal Officer*

Evanthia CHATZILIASI  
*Legal Officer*

Graça COSTA  
*Legal Officer*

Fanny COUDERT  
*Legal Officer*

Andy GOLDSTEIN  
*Legal and Technical Officer*

Xanthi KAPSOSIDERI  
*Legal Officer*

Anna LARSSON STATIN\*  
*Legal Officer*

Adeline MORRIS  
*Legal Officer*

Anne NOEL  
*Supervision & Enforcement Assistant*

Lara SMIT  
*Legal Officer*

Snezana SRDIC  
*Legal Officer*

Tereza STRUNCOVA  
*Legal Officer*

Zsofia SZILVASSY  
*Legal Officer*

Jeroen WAUMAN  
*Legal Officer*

Anna ZAWILA-NIEDZWIECKA  
*Legal Officer*

Aikaterini POULIOU  
*Legal Officer*

Priscilla DE LOCHT  
*Legal Officer*

Joanna PARKIN  
*Legal Officer*

Michal FILA  
*Legal Officer*

## Policy and Consultation

Anna BUCHTA  
*Head of Unit*

Olivier MATTER  
*Head of International Cooperation*

Plamen ANGELOV  
*Head of Justice and Home Affairs*

Chikezie AGUBUZU  
*Policy and Consultation Assistant*

## ANNEXES

Veronique CIMINA  
*Legal Officer*

Mario GUGLIELMETTI  
*Legal Officer*

Amanda JOYCE\*  
*Policy and Consultation Assistant*

Claire- Agnes MARNIER  
*Legal Officer*

Romain ROBERT\*  
*Legal Officer*

Niksa STOLIC  
*Legal Officer/ Seconded National Expert*

Agnieszka ZAPOROWICZ  
*Legal Officer*

Brendan VAN ALSENOY  
*Legal Officer*

Sonia PEREZ ROMERO  
*Legal Officer*

Leda BARGIOTTI  
*Legal Officer*

Geoffrey DEVIN  
*Legal Officer*

Dina KAMPOURAKI  
*Technology and Security Officer*

Georgios KOTSAKIS  
*Technology and Security Officer*  
*LISO*

Xabier LAREO  
*Technology and Security Officer*

Frederik LINDHOLM  
*Administrative Assistant*

Lukasz OLEJNIK\*  
*Technology and Security Officer*

Robert RIEMANN  
*Technology and Security Officer*

Konstantina VEMOU  
*Technology and Security Officer*

Karim SGAIER  
*Administrative Assistant*

Alexandre LEAO  
*Technology and Security Officer*

Vitor BERNARDO  
*Technology and Security Officer*

Stefano LEUCCI  
*Technology and Security Officer*

## Technology and Privacy

Thomas ZERDICK  
*Head of Unit*

Massimo ATTORESI  
*Deputy Head of Unit*

## Records Management Sector

Luisa PALLA  
*Head of Sector*

Marta CÓRDOBA HERNÁNDEZ  
*Administrative Assistant*

Kim Thien LÊ  
*Administrative Assistant*

Vincenza MINIELLO  
*Administrative Assistant*

Alison PROCTER  
*Administrative Assistant*

Maria TIGANITAKI  
*Administrative Assistant*

Martine VERMAUT  
*Administrative Assistant*

Lucia MARTINEZ SEBASTIAN  
*Records and Archive Manager*

Constantino MONTES Y CAMINO  
*Finance and Procurement Officer*

## Human Resources, Budget and Administration

Marian SANCHEZ LOPEZ  
*Head of Unit*

Karina REMPESZ  
*Deputy Head of Unit*

Kim BUI  
*Head of Finance*

Anne-Françoise REYNDERS  
*Head of Human Resources*

Cláudia BEATO  
*HR Assistant*

Pascale BEECKMANS  
*HR Assistant*

Laetitia BOUAZZA  
*HR Assistant*  
*Traineeship Coordinator*

Angelo FASSARI  
*Procurement Assistant*

Sebastian GALEA  
*Finance Assistant*

Sophie JEANNON  
*Administrative Assistant*

Sophie LOUVEAUX  
*Trainer and Internal Coach*

## Information and Communication

Olivier ROSSIGNOL  
*Head of Sector*

Agnieszka NYKA  
*Deputy Head of Sector*

Francesco ALBINATI  
*Information & Communication Officer*

Thomas HUBERT  
*Graphic Designer Assistant*

Courtenay MITCHELL\*  
*Information and Communication Officer*

Parminder MUDHAR  
*Information and Communication Officer*

Julia HODDER  
*Information and Communication Officer*

## ANNEXES

Marco MORESCHINI  
*HR Officer/ Seconded National Expert*  
LSO

Jean-Michel VERSTAEN  
*Finance Assistant*

Francoise MAYEUR  
*HR Assistant-Assistant to Head of Unit and Human Resources*

Aidas GLEMZA  
*Administrative Assistant*

### EDPB Secretariat

Isabelle VEREECKEN  
*Head of the EDPB Secretariat*

Greet GYSEN  
*Head of External Communication matters*

Ahmed IMMOUN  
*Head of IT matters*

Effrosyni PANAGOU  
*Head of Administrative matters*

Katinka BOJNAR  
*Legal Officer*

Hannelore DEKEYSER  
*Legal Officer*

Carolina FOGLIA  
*Legal Officer*

Sarah HANSELAER  
*Information and Communications Officer*

Joelle JOURET\*  
*Legal Officer*

Peter KRAUS  
*Technology and Security Officer*  
LISO

Fabienne MOLLET  
*Administrative Assistant*

Veronica MORO  
*Project Officer*

Nerea PERIS BRINES  
*Legal Officer*

João SILVA  
*Legal Officer*  
DPO

Constantin STANCU\*  
*Archivist*

Jasminka TOKALIC\*  
*Administrative Assistant*

Anne- Marie VANDENBERGHEN\*  
*Administrative Assistant*

Michal CZERNIAWSKI  
*Legal Officer*

Ignacio GOMEZ NAVARRO  
*Legal Officer*

Myriam GUFFLET  
*Legal Officer*

Anna LYTRA  
*Legal Officer*

Marie-Francoise DEMARCQ  
*Administrative Assistant*



Paola CASINI  
*Records and Archive Manager*

Marie McGINLEY  
*Legal Officer*

Georgios ZISIS  
*Administrative Assistant*

Gianna DASKALAKI  
*Administrative Assistant*

Joaquín SILGUERO  
*Legal Officer / Seconded National Expert*

Gintare PAZERECKAITE  
*Legal Officer*

*\*Members of EDPS staff that left the organisation in 2020.*

# 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.



edps.europa.eu



Twitter:

@EU\_EDPS



Linkedin:

EDPS



Youtube:

European Data Protection Supervisor

Email address:

edps@edps.europa.eu



Publications Office  
of the European Union

