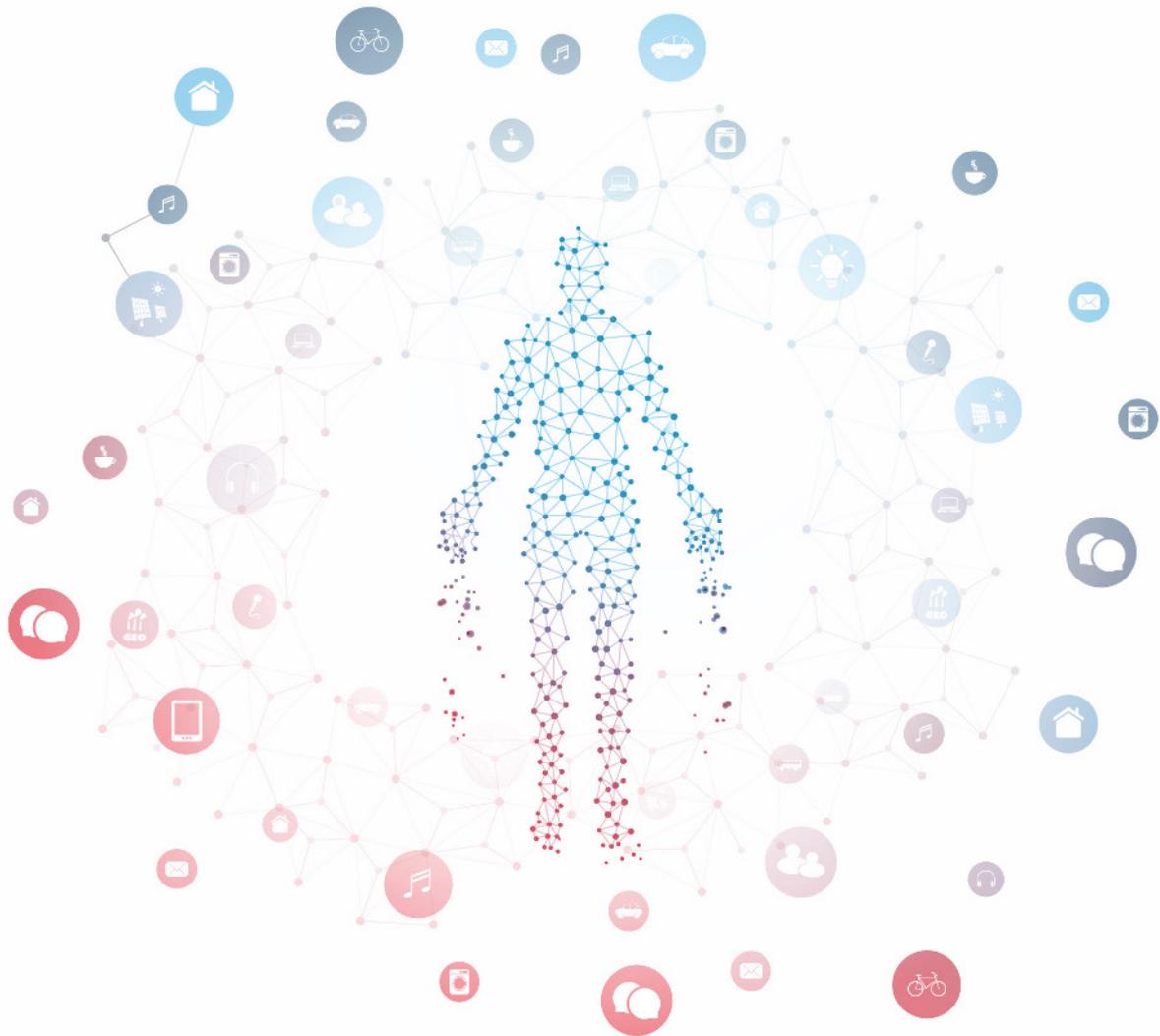




# EUROPEAN DATA PROTECTION SUPERVISOR



ANNUAL  
**REPORT**  
2018

An Executive Summary of this report, which gives an overview of key developments in EDPS activities in 2018, is also available.

Further details about the EDPS can be found on our website at <http://www.edps.europa.eu>.

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

Luxembourg: Publications Office of the European Union, 2019

© Photos: iStockphoto/EDPS & European Union

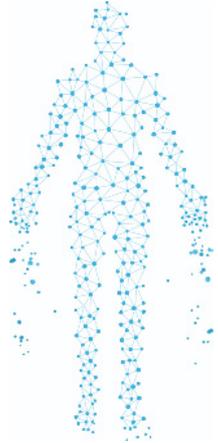
© European Data Protection Supervisor, 2019

Reproduction is authorised provided the source is acknowledged.

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

PDF	ISBN 978-92-9242-280-6	ISSN 1830-9585	doi:10.2804/801791	QT-AA-19-001-EN-N
Print	ISBN 978-92-9242-282-0	ISSN 1830-5474	doi:10.2804/17012	QT-AA-19-001-EN-C
HTML	ISBN 978-92-9242-281-3	ISSN 1830-9585	doi:10.2804/793717	QT-AA-19-001-EN-Q

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)



ANNUAL  
**REPORT**

---

2 0 1 8

EUROPEAN DATA PROTECTION SUPERVISOR



# | Contents

▶ <b>FOREWORD</b>	<b>5</b>
▶ <b>MISSION STATEMENT, VALUES AND PRINCIPLES</b>	<b>7</b>
▶ <b>EDPS STRATEGY 2015-2019</b>	<b>8</b>
<b>1. About the EDPS</b>	<b>9</b>
<b>1.1 Supervision and Enforcement</b>	<b>9</b>
<b>1.2 Policy and Consultation</b>	<b>10</b>
<b>1.3 Monitoring technological developments</b>	<b>10</b>
<b>2. 2018 - An Overview</b>	<b>11</b>
<b>2.1 New legislation for a new era</b>	<b>11</b>
<b>2.2 Finding a balance between security and privacy</b>	<b>12</b>
<b>2.3 Developing partnerships</b>	<b>12</b>
<b>2.4 Digital Ethics and the International Conference</b>	<b>13</b>
<b>2.5 Internal administration</b>	<b>13</b>
<b>2.6 Communicating data protection</b>	<b>13</b>
<b>2.7 Key Performance Indicators 2018</b>	<b>14</b>
<b>3. Main Objectives for 2019</b>	<b>16</b>
<b>4. 2018 Highlights</b>	<b>19</b>
<b>4.1 Preparing for a new legislative framework</b>	<b>19</b>
4.1.1 The EDPB gets to work	20
4.1.2 The data protection Regulation for EU institutions	21
4.1.3 ePrivacy: completing the EU's data protection framework	22
4.1.4 Privacy by Design: technology that serves the people	25
<b>4.2 Supervising Europol</b>	<b>25</b>
4.2.1 Continuous cooperation with Europol's data protection unit	25
4.2.2 Supervising operational analysis projects	26
4.2.3 Inspecting Europol	26
4.2.4 Advising Europol	27
4.2.5 Dealing with complaints	28
4.2.6 Meeting with the Cooperation Board	28
4.2.7 Setting the tone at management level	29
4.2.8 The Joint Parliamentary Scrutiny Group	29
<b>4.3 Security and EU borders</b>	<b>30</b>
4.3.1 Effective supervision of large-scale IT systems	30
4.3.2 Coordinated supervision of large-scale IT systems	31

4.3.3	Observing Schengen	31
4.3.4	Protecting fundamental rights in the area of freedom, security and justice	32
<b>4.4.</b>	<b>On the ground</b>	<b>34</b>
4.4.1	The DPO function: EU institutions leading by example	35
4.4.2	Reinforcing the accountability of EU institutions	36
4.4.3	Accountability in IT	36
4.4.4	Data breach notifications: a how-to guide for EU institutions	37
4.4.5	Protecting privacy in the EU institutions	37
4.4.6	Catching up with the institutions: audits and visits	43
4.4.7	Remote inspections of webservices	43
4.4.8	Transparency, re-use and data protection	44
4.4.9	Cross-border investigations of a different kind	44
4.4.10	Application for Return	45
4.4.11	Security verifications of external contractors	45
4.4.12	Supervising the EFTA Surveillance Authority	45
4.4.13	Eurojust: a new supervisory role for the EDPS	46
4.4.14	Advising the EU institutions	46
4.4.15	New technologies	48
4.4.16	Privacy engineering gaining ground	48
4.4.17	Online manipulation and personal data	49
4.4.18	A more coherent approach to challenges in the digital ecosystem: The Digital Clearinghouse	50
<b>4.5.</b>	<b>International affairs</b>	<b>50</b>
4.5.1	International data transfers	51
4.5.2	International cooperation	51
<b>4.6</b>	<b>Digital Ethics</b>	<b>53</b>
4.6.1	The Ethics Advisory Group: Reporting on Digital Ethics	54
4.6.2	Getting your views on Digital Ethics	54
4.6.3	Encouraging debate around the world	55
<b>4.7</b>	<b>The 2018 International Conference of Data Protection and Privacy Commissioners</b>	<b>56</b>
4.7.1	The Closed Session - Ethics and Artificial Intelligence	56
4.7.2	The Public Session - Debating Ethics	57
4.7.3	Side Events	59
4.7.4	Social Events	59
4.7.5	Conference Communication	60

## 5. Court Cases 62

## 6. Transparency and Access to Documents 63

## 7. The Secretariat 64

<b>7.1</b>	<b>Information and Communication</b>	<b>64</b>
7.1.1	Online media	64
7.1.2	Events and publications	65
7.1.3	External relations	67
7.1.4	The EDPB	68
<b>7.2</b>	<b>Administration, Budget and Staff</b>	<b>68</b>
7.2.1	Budget and finance	68
7.2.2	Preparing for the EDPB secretariat	69
7.2.3	A competition for data protection specialists	70
7.2.4	The GDPR for EUI: HR preparations	70
7.2.5	Improving HR policies	70

<b>8. The Data Protection Officer at the EDPS</b>	<b>72</b>
<b>8.1 The DPO at the EDPS</b>	<b>72</b>
<b>8.2 The transition to a new Regulation</b>	<b>72</b>
<b>8.3 Advising the institution and improving the level of protection</b>	<b>73</b>
<b>8.4 Enquiries and complaints</b>	<b>73</b>
<b>8.5 Awareness-raising within the EDPS</b>	<b>73</b>
<b>8.6 Collaboration with DPOs in the other EU institutions</b>	<b>73</b>
<b>Annex A - Legal framework</b>	<b>74</b>
<b>Annex B - Extract from Regulation (EU) 2018/1725</b>	<b>77</b>
<b>Annex C – List of Data Protection Officers</b>	<b>80</b>
<b>Annex D - List of prior check and non-prior check opinions</b>	<b>82</b>
<b>Annex E – List of Opinions and formal comments on legislative proposals</b>	<b>85</b>
<b>Annex F – Speeches by the Supervisor and Assistant Supervisor in 2018</b>	<b>86</b>
<b>Annex G - Composition of EDPS Secretariat</b>	<b>90</b>

## **TABLES AND GRAPHS**

<b>Figure 1.</b> EDPS KPI analysis table	<b>15</b>
<b>Figure 2.</b> EDPS training programme 2018	<b>23</b>
<b>Figure 3.</b> Evolution of the number of complaints, including inadmissible complaints, received by EDPS	<b>39</b>
<b>Figure 4.</b> EU institutions and bodies concerned by complaints received by EDPS	<b>39</b>
<b>Figure 5.</b> Type of violation alleged in complaints received by EDPS	<b>40</b>
<b>Figure 6.</b> Evolution of Notifications received by EDPS	<b>41</b>
<b>Figure 7.</b> Evolution of prior check Opinions issued by EDPS	<b>41</b>
<b>Figure 8.</b> Percentage split between Core Business and Administration activities in the Notifications received by EDPS	<b>42</b>



## | Foreword

2018 demonstrated the power and the limitations of data protection.

Two years after its adoption, on 25 May 2018 the General Data Protection Regulation (GDPR) became fully applicable.

People noticed because they were bombarded with identikit emails, each informing them of an updated privacy policy and, in most cases, requesting that they accept it to continue using the service. So far, rather than adapting their way of working to better protect the interests of those who use their services, companies seem to be treating the GDPR more as a legal puzzle, in order to preserve their own way of doing things.

We should expect this to change over the coming year, however.

The biggest threat to individual freedom and dignity stems from the excessive informational power of certain companies, or controllers, and the wider, incompressible ecosystem of trackers, profilers and targeters that are able to gather and use this information.

Just three months before the GDPR became fully enforceable, the abuse of personal data became headline news and the subject of official enquiries, not only in the European Parliament, but also in national capitals, from Washington DC to London to Delhi. Public policymakers are now very much alive to the threat the current situation poses, not just to the freedom of consumers in the eCommerce environment, but also to democracy itself.

The whole system is susceptible, not only to breaches, but also to manipulation by actors with political agendas aiming to undermine trust and societal cohesion. The litmus test of how robust the EU's legal regime really is will be the integrity of the European Parliament Elections in 2019.

Coherent enforcement of all rules, including data protection, to prevent and punish unlawful interference during the elections, will be vitally important. We therefore deeply regret the delay in the adoption of updated rules on ePrivacy. Without these updated rules to ensure respect for the most intimate, sensitive information and private communications, companies and individuals remain exposed and vulnerable, subject to a patchwork of EU laws and legal uncertainty which fail to provide us with control over our own digital selves.

Nevertheless, the EU data protection reform agenda scored one major win before the end of the year. On 11 December 2018, the entry into force of a GDPR for the EU institutions ensured that all 66 of the EU institutions and bodies that we supervise, as well as the EDPS itself, are now subject to the same rigour as controllers under the GDPR.

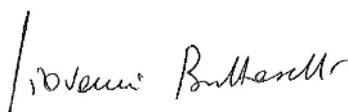
After two years of intense preparation, during which we have worked in close cooperation not only with our data protection counterparts in the institutions, but also with top management and other EU employees, the EU institutions are now able to lead by example in their implementation of data protection rules.

At the International Conference of Data Protection and Privacy Commissioners in October, we had the honour of showcasing the EU's commitment to ethics and human dignity. The world's data protection authorities led the way in scrutinising the human impact of artificial intelligence, while an extraordinarily rich and diverse collection of voices from around the world came together at the public session of the conference to discuss how technology is disrupting our lives and to call for a new consensus on what is right and wrong in the digital space. We will continue to facilitate this conversation in 2019 and beyond.

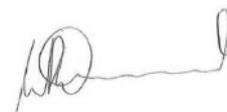
On a global scale, data protection continues to demonstrate its geostrategic importance. We see this in the ongoing debate on the Privacy Shield and the imminent (reciprocated) decision on the *adequacy* of data protection safeguards in Japan. We also see it in the importance given to data protection in the law enforcement community. Our role as a hands-on regulator of the European Police Agency, Europol, is now well-established, while at the end of 2019 we will take on a similar role for the EU's judicial cooperation unit, Eurojust.

The new European Data Protection Board (EDPB), which began its work on 25 May 2018, faces an enormous challenge to prove that 29 independent authorities can act as one, respecting one another's approaches and methods but converging towards a recognisably and reliably credible European enforcement culture. We are delighted that the secretariat provided by the EDPS was fully functional from day one of the GDPR and will continue to provide support where we are able to do so.

Wojciech and I are now in the final year of our mandate. In March 2015, we published a Strategy setting out our vision, objectives and action points for the years to come. In the coming months, we will publish a review of our efforts in relation to the Strategy, ensuring that we hold ourselves accountable to the targets we set back in 2015.



**Giovanni Buttarelli**  
European Data Protection Supervisor



**Wojciech Wiewiórowski**  
Assistant Supervisor

# | Mission statement, values and principles

Data protection is a fundamental right, protected by European law and enshrined in Article 8 of the [Charter of Fundamental Rights of the European Union](#).

In order to protect and guarantee the rights to data protection and privacy, the processing of personal data is subject to control by an independent authority. The European Data Protection Supervisor (EDPS) is the European Union's independent data protection authority, tasked with ensuring that the institutions and bodies of the EU respect data protection law.

In accordance with [Regulation 2018/1725](#), and with [Regulation 45/2001](#) previously, the EU as a policy making, legislating and judicial entity looks to the EDPS as an independent supervisor and impartial advisor on policies and proposed laws which might affect the rights to privacy and data protection. The EDPS performs these functions by establishing itself as a centre of excellence in the law, and also in technology, insofar as it affects or is affected by the processing of personal data.

We carry out our functions in close cooperation with fellow data protection authorities as part of the European Data Protection Board (EDPB), and aim to be as transparent as possible in our work serving the EU public interest. Under the [General Data Protection Regulation](#), the EDPS is also responsible for providing the secretariat to the EDPB.

Our approach to our tasks and the way in which we work with our stakeholders are guided by the following values and principles:

## Core values

- **Impartiality** – working within the legislative and policy framework given to us, being independent and objective, finding the right balance between the interests at stake.
- **Integrity** – upholding the highest standards of behaviour and doing what is right even if it is unpopular.
- **Transparency** – explaining what we are doing and why, in clear language that is accessible to all.
- **Pragmatism** – understanding our stakeholders' needs and seeking solutions that work in practice.

## Guiding principles

- We serve the public interest to ensure that EU institutions comply with data protection principles in practice. We contribute to wider policy as far as it affects European data protection.
- Using our expertise, authority and formal powers, we aim to build awareness of data protection as a fundamental right and as a vital part of good public policy and administration for EU institutions.
- We 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. We act selectively and proportionately.

# | EDPS Strategy 2015-2019

The [EDPS Strategy 2015-2019](#) was adopted on 2 March 2015, at the beginning of the current EDPS mandate. It defines our priorities and informs our work by providing a framework through which to promote a new culture of data protection in the European institutions and bodies.

## About the Strategy

At the beginning of his mandate in 2015, the new EDPS finalised a strategy for the coming five years. His aim was to realise his vision of an EU that leads by example in the debate on data protection and privacy and to identify innovative solutions quickly.

The 2015-2019 strategic plan summarises:

- the major data protection and privacy challenges over the course of the mandate;
- three strategic objectives and ten accompanying actions for meeting those challenges;
- how to deliver the strategy, through effective resource management, clear communication and evaluation of our performance.

Our aims and ambitions build on our strengths, successes and the lessons learned from implementing our [Strategy 2013-2014: Towards Excellence in Data Protection](#).

## Vision, Objectives and Action 2015-2019

Our vision is to help the EU lead by example in the global dialogue on data protection and privacy in the digital age. Our three strategic objectives and ten actions are:

- 1 Data protection goes digital
  - (1) promoting technologies to enhance privacy and data protection;
  - (2) identifying cross-disciplinary policy solutions;
  - (3) increasing transparency, user control and accountability in big data processing.

- 2 Forging global partnerships
  - (4) developing an ethical dimension to data protection;
  - (5) speaking with a single EU voice in the international arena;
  - (6) mainstreaming data protection into international policies.
- 3 Opening a new chapter for EU data protection
  - (7) adopting and implementing up-to-date data protection rules;
  - (8) increasing the accountability of EU bodies collecting, using and storing personal information;
  - (9) facilitating responsible and informed policymaking;
  - (10) promoting a mature conversation on security and privacy.



@EU\_EDPS

**#EDPS** strategy envisions **#EU** as a whole not any single institution, becoming a beacon and leader in debates that are inspiring at global level

# | 1. About the EDPS

The EDPS ensures that the European institutions and bodies respect the fundamental rights to privacy and data protection, whether they are involved in processing personal data or in developing new policies. We have three 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 prior checking processing operations likely to present specific risks, to handling complaints and conducting inquiries.
- **Consultation:** We advise the European Commission, the European Parliament and the Council on proposals for new legislation and other initiatives related to data protection.
- **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).

Up until 11 December 2018, the EU institutions had to comply with the data protection rules set out in [Regulation 45/2001](#), which the EDPS was required to enforce. On 11 December 2018, these rules were replaced by [Regulation 2018/1725](#).

Regulation 2018/1725 is the EU institutions' 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 that all other organisations operating in the EU must comply with. It also tasks the EDPS with providing the secretariat for the EDPB.

In addition to this, separate rules exist concerning the processing of personal data for operational activities carried out by the EU's law enforcement agency, Europol. These activities include the fight against serious crime and terrorism affecting more than one Member State. The relevant legislation in this case is [Regulation 2016/794](#), which also provides for EDPS supervision of these data processing activities.

## 1.1 SUPERVISION AND ENFORCEMENT

The EDPS aims to ensure that EU institutions are not only aware of their data protection obligations, but can

also be held accountable for complying with them. We have several tools we can use, all of which are aimed at encouraging the development of a data protection culture in the EU institutions:

- **Prior checks/Prior consultations:** Under Regulation 45/2001, EU institutions and bodies had to inform the EDPS of any procedure they planned to carry out which might have posed a risk to the protection of personal data. We examined the proposals and provided recommendations on how to address these risks. Under the new Regulation, prior checks no longer exist in this form. However, in certain cases, EU institutions and bodies must consult the EDPS after carrying out a data protection impact assessment for a planned risky procedure.
- **Complaints:** We handle complaints from individuals relating to the processing of personal data by the EU institutions. We investigate these complaints and decide on the best way to handle them.
- **Monitoring compliance:** The EDPS is responsible for ensuring that all EU institutions and bodies comply with data protection rules. We monitor compliance in various ways, including through visits and [inspections](#).
- **Consultations on administrative measures:** We issue Opinions on administrative measures relating to the processing of personal data, either in response to a specific request from an EU institution or on our own initiative.
- **Guidance:** We issue [Guidelines](#) for the EU institutions, designed to help them better implement data protection principles and comply with data protection rules.
- **Working with Data Protection Officers (DPOs):** Each EU institution and body must appoint a DPO, who is responsible for ensuring that their institution complies with data protection rules. We work closely with DPOs, providing them with training and support to help them perform their role effectively.
- **Training the EU institutions and bodies:** We provide training sessions for managers and staff members of the EU institutions and bodies. 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 institution. These training sessions focus on helping institutions to go beyond compliance and demonstrate accountability.

## 1.2 POLICY AND CONSULTATION

The EDPS acts as an advisor on data protection issues to the EU legislator. 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. We use several tools to help us:

- **Informal Comments:** In line with established practice, the Commission consults the EDPS informally before adopting a proposal with implications for data protection. This allows us to provide them with input at an early stage of the legislative process, usually in the form of informal comments, which are not published.
- **Opinions:** Our formal Opinions are available on our website and are published in the Official Journal of the EU. We use them to highlight our main data protection concerns and recommendations on legislative proposals. They are addressed to all three EU institutions involved in the legislative process.
- **Formal Comments:** Like our Opinions, our formal Comments address the data protection implications of legislative proposals. However, they are usually shorter and more technical, or only address certain aspects of a proposal. We publish them on our website.
- **Court Cases:** We can intervene and offer our data protection expertise before the EU courts either on behalf of one of the parties in a case or at the invitation of the Courts.
- **Cooperation with national DPAs:** We cooperate with national DPAs through the EDPB, which ensures the consistent application of the GDPR through guidelines, recommendations and best practices, opinions and binding decisions, and provides the European Commission with advice on data protection issues. We also work with national DPAs to ensure a consistent and coordinated approach to the supervision of a number of EU databases.

## 1.3 MONITORING TECHNOLOGICAL DEVELOPMENTS

Many new technologies process personal data in a range of different and innovative ways. The aim of this data

processing is often to gain economic or other benefits. Data protection and privacy measures must adequately address new technological developments. This will ensure that individuals are protected from the risks these new data processing activities might entail.

The EDPS monitors technological developments and their impact on data protection and privacy. Knowledge and expertise in this area allows us to effectively perform our supervision and consultation tasks. This capacity and competence will only continue to grow in importance, due to the changes introduced by the GDPR and the new Regulation for the EU institutions and bodies. 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 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 which incorporate privacy concerns and 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 2018/1725 now fully applicable, it has become a legal obligation for all controllers to take account of the state of the art of 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, it is important that DPAs establish a common understanding of the state of the art and its development. With this in mind, the EDPS cooperates with the national supervisory authorities to assess and evaluate existing and developing technological and organisational options.
- **Keeping track of IT at the EDPS:** As the data protection supervisor for the EU institutions, we should set the standard for data protection compliance. We therefore continually monitor and improve the technology used by the EDPS to ensure that it works effectively and efficiently while remaining in line with data protection requirements.

## | 2. 2018 - An Overview

In the [EDPS Strategy 2015-2019](#), we outline a vision of an EU that leads by example in the global dialogue on data protection and privacy in the digital age. We set ourselves a challenging and ambitious agenda, which we have sought to carry out over the course of the current mandate.

We made great strides towards achieving these goals in 2018, a year which could be considered pivotal both in the history of data protection and in the history of the EDPS.

### 2.1 NEW LEGISLATION FOR A NEW ERA

One of the three objectives set out in our Strategy was to open a new chapter for EU data protection. Technological development is moving at a rapid pace and the way in which we live, as individuals and as a society, is also changing rapidly to accommodate this. Logically, the EU's data protection rules also required an update, not aimed at slowing down innovation, but at ensuring that individuals' fundamental rights are protected in the digital era.

On 25 May 2018, new data protection legislation became fully applicable to all companies and organisations operating in the EU Member States. The [General Data Protection Regulation](#) (GDPR) marked the first step towards ensuring comprehensive and effective protection of personal data and privacy for all individuals in the EU.

With this new legislation came the establishment of the European Data Protection Board (EDPB) ([see section 4.1.1](#)). Made up of the 28 EU Member State [data protection authorities](#) (DPAs) and the EDPS, this new body is entrusted with ensuring the consistent implementation of the GDPR across the EU. Charged with providing the secretariat for this new EU body, a significant amount of our time and effort in early 2018 went into ensuring that the Board would be prepared to deal with its heavy workload from day one of the new Regulation. We have continued to support the EDPB secretariat administratively throughout the year, as well as participating fully as a member of the Board itself.

We moved yet another step closer to achieving a comprehensive framework for data protection with the adoption of new rules for the EU institutions and bodies. [Regulation 2018/1725](#) came into force on 11 December

2018, bringing the rules for the EU institutions in line with the rules set out in the GDPR ([see section 4.1.2](#)).

As the supervisory authority for data protection in the EU institutions and bodies, we faced the significant challenge of ensuring that they were all prepared for these new rules. In 2017, we embarked on a campaign of visits, training sessions and meetings ([see figure 2](#)), which intensified over the course of 2018. These were aimed at raising awareness and about the new rules and helping to ensure that the EU institutions had the knowledge and tools to put them into practice.

A specific focus of these activities was on encouraging the development of a culture of [accountability](#) within the EU institutions. We wanted to ensure that they not only comply with data protection rules, but that they can demonstrate this compliance. Integral to this was creating awareness that the processing of personal data, even when done lawfully, can put the rights and freedoms of individuals at risk. These activities will continue into 2019, as we endeavour to ensure that the EU institutions lead the way in the application of new data protection rules.

The misuse of personal data for tracking and profiling purposes and the role of technology in our society was a topic of significant public debate in 2018. The EDPS and the data protection community in general were at the forefront of this debate, with the EDPS contributing on two main fronts: through our [Opinion](#) on online manipulation and personal data ([see section 4.4.17](#)) and our [Opinion](#) on Privacy by Design ([see section 4.1.4](#)).

While the former focused on the need to extend the scope of protection afforded to individuals' interests in today's digital society, the latter looked to address the new challenges resulting from technological and legal developments. On the legal side, the new generation of data protection rules laid down in the GDPR, Directive 2016/680 and Regulation 2018/1725 on the processing of personal data by EU institutions requires that controllers take account of the state of the art in technical and organisational measures to implement data protection principles and safeguards. This also requires that supervisory authorities are aware of the state of the art in this domain and that they follow its development. Cooperation in this field is of crucial importance in order to ensure that these principles are applied consistently. The Opinion also built on our work with the [Internet Privacy Engineering Network](#) (IPEN)

(see section 4.4.16) to encourage dialogue between policymakers, regulators, industry, academia and civil society on how new technologies can be designed to benefit the individual and society.

The new data protection rules also introduce the principle of accountability (see section 4.4.2). All controllers, including the EU institutions and bodies, must ensure that they are able to demonstrate compliance with the new rules. This also applies to the management and governance of their IT infrastructure and systems. To help with this, we extended our catalogue of specific guidelines to include, among others, [Guidelines on the use of cloud computing services](#) by the EU administration and further [guidance on IT management and IT governance](#) (see section 4.4.3). In 2018, we also began a systematic programme aimed at verifying EU bodies' compliance with EDPS guidelines.

## 2.2 FINDING A BALANCE BETWEEN SECURITY AND PRIVACY

1 May 2018 marked one year since the EDPS took over responsibility for supervising the processing of personal data for operational activities at the EU's law enforcement agency, Europol. One of the action points set out in our Strategy as integral to opening a new chapter for data protection in the EU is to promote a mature conversation on security and privacy. As an EU agency charged with ensuring the security of the EU while protecting the fundamental rights to privacy and data protection, Europol is a great example of the progress we are making in this area (see section 4.2).

We continue to maintain a strong relationship with Europol's [Data Protection Officer](#) (DPO) and Data Protection Function (DPF) Unit, which allows us to anticipate any possible problems and plan future activities (see section 4.2.1). We carried out our second inspection of data processing activities at the agency in May 2018 (see section 4.2.3) and continued to provide advice and deal with complaints where required (see sections 4.2.4 and 4.2.5).

The security of EU borders remains a hot topic and the EU legislator put forward several new proposals in 2018 aimed at increasing security and improving border management. While we recognise the need for greater EU security, this should not come at the expense of data protection and privacy.

Facilitating responsible and informed policymaking is another of the action points required in order to open a new chapter in EU data protection. With this in mind we issued several Opinions on proposed EU border policy

in 2018 (see section 4.3.4). One of these focused on the future of information sharing in the EU, addressing Proposals for two Regulations which would establish a framework for interoperability between [EU large-scale information systems](#). As the implications of this proposal for data protection and other fundamental rights and freedoms are uncertain, we will launch a debate on this issue in early 2019 to ensure they are explored in detail.

We also continued our close cooperation with DPAs to ensure effective and coordinated supervision of the EU's large-scale IT databases, used to support EU policies on asylum, border management, police cooperation and migration (see sections 4.3.1 and 4.3.2).

## 2.3 DEVELOPING PARTNERSHIPS

Facilitating responsible and informed policymaking is far from limited to the field of EU security and border policy, however. In 2018, the EDPS issued 11 Opinions, including two upon request from the Council, on matters ranging from jurisdiction in matrimonial matters to the interoperability of EU large-scale information systems.

We also issued 14 sets of formal comments. These are equivalent to Opinions, but typically shorter and more technical. Some of our comments were expressly requested by the European Parliament, or one of its Committees, and concerned not the initial legislative proposals, but draft amendments and outcomes of negotiations between the co-legislators.

Taking into account that we also dealt with over 30 informal consultations on draft proposals by the Commission, these numbers clearly demonstrate the increased need for, and relevance of, independent expert advice on the data protection implications of EU initiatives, as well as growing interest from EU institutional stakeholders. We look forward to continuing this mutually beneficial cooperation in the coming years in the context of strengthened legislative consultation powers under the new Regulation 2018/1725.

We also continued our efforts to ensure that activities within the EU institutions are carried out in accordance with the relevant data protection laws, issuing prior-check Opinions, investigating complaints and monitoring compliance through the various tools available to us (see section 4.4).

The Strategy commits the EDPS to forging partnerships in pursuit of greater data protection convergence globally. While data flows internationally, across borders, data protection rules are decided on a largely national, and at best regional, basis.

With this in mind, we continue to work with our regional and international partners to mainstream data protection into international agreements and ensure consistent protection of personal data worldwide (see section 4.5.2).

We are also involved in discussions on adequacy findings. These agreements are made by the European Commission on behalf of the EU Member States, and provide for the transfer of data from EU countries to non-EU countries whose data protection rules are deemed to provide adequate protection. Specifically, in 2018, we contributed to the second joint review of the EU-US Privacy Shield and the EDPB Opinion on a proposed adequacy agreement with Japan (see section 4.5.1).

## 2.4 DIGITAL ETHICS AND THE INTERNATIONAL CONFERENCE

We launched the [EDPS Ethics Initiative](#) back in 2015, as part of our commitment to forging global partnerships. We wanted to generate a global discussion on how our fundamental rights and values can be upheld in the digital era.

Three years on and digital ethics is now very much on the international agenda.

We began 2018 with the publication of the [Ethics Advisory Group Report](#) (see section 4.6.1). The Report is a useful tool in helping us to understand how the digital revolution has changed the way we live our lives, both as individuals and as a society. It also outlines the changes and challenges this implies for data protection. From here, we were able to expand our enquiry to reach a much larger audience, through a public consultation launched in early summer 2018 (see section 4.6.2). The results of the consultation revealed the importance of ethics moving forward and called for DPAs to play a proactive role in this.

However, it was the [International Conference of Data Protection and Privacy Commissioners](#), dubbed the *Olympic Games of Data Protection* by EDPS Giovanni Buttarelli, that really launched the discussion on digital ethics onto the international agenda.

The public session of the International Conference focused on *Debating Ethics: Dignity and Respect in Data Driven Life*. With over 1000 people from a variety of different backgrounds, nationalities and professions in attendance, high-profile speakers and considerable media coverage, the event served to foster debate on the issue and put new ethical and legal questions high on the agenda of DPAs and others across the world.

The EDPS is now seen as a leader in this area and will work hard to progress the debate (see section 4.7).

## 2.5 INTERNAL ADMINISTRATION

With our role and responsibilities expanding, good internal administration has been more important than ever in ensuring that we are able to achieve our goals.

The EDPS Human Resources, Budget and Administration (HRBA) Unit tackled two particularly big preparatory tasks in 2018 (see section 7.2). Work on preparations for the new EDPB secretariat intensified significantly in order to ensure that the Board was administratively and logistically prepared to start work on 25 May 2018. Among other things, this involved ensuring that all EDPB staff members were subject to the same rules as those working for the EDPS and able to benefit from the same rights.

Ahead of the new data protection Regulation for the EU institutions, we also had to ensure that all EDPS HR decisions complied with the new rules. We therefore undertook a full review of all EDPS HR data processing activities and revised our approach as needed.

In addition to a number of initiatives aimed at improving our HR policies, we launched a new open competition to create a pool of highly qualified data protection experts to satisfy our future recruitment needs. As we move into 2019, our main aim is to ensure an efficient and pleasant work environment for all those who work at the EDPS.

## 2.6 COMMUNICATING DATA PROTECTION

The importance of EDPS communication activities has increased considerably over the past few years (see section 7.1). Effective communication is essential in ensuring that we are able to achieve the goals set out in our Strategy. If our work is not visible, it cannot have the impact required.

In addition to consolidating our efforts to improve and increase the impact of our online presence, we launched and executed two communication campaigns. Our communication efforts for the 2018 International Conference not only helped to ensure that the conference itself was a success, but that the debate on digital ethics reached the widest possible audience.

In December 2018, we turned our attention to the new data protection Regulation for the EU institutions. Our communication campaign was designed to complement

and reinforce ongoing awareness-raising activities, it was aimed not only at EU staff members, but also at ensuring that people outside the EU institutions were aware of the new rules and how they might affect them.

With the global presence and influence of the EDPS only set to increase, we anticipate another busy year ahead in 2019.

## 2.7 KEY PERFORMANCE INDICATORS 2018

We use a number of key performance indicators (KPIs) to help us monitor our performance. This ensures that we are able to adjust our activities, if required, to increase the impact of our work and the efficiency of our use of resources. These KPIs reflect the strategic objectives and action plan defined in our Strategy 2015-2019.

The KPI scoreboard below contains a brief description of each KPI and the results on 31 December 2018. In most cases, these results are measured against initial targets.

In 2018, we met or surpassed, in some cases significantly, the targets set in the majority of our KPIs. This shows that implementation of the relevant strategic objectives is well on track and no corrective measures are needed.

In two cases we do not have monitoring results. In the case of KPI 6, in the course of 2018 we opted to monitor and prioritise our policy activities in relation to the relevant priority actions outlined in our Strategy, instead of publishing a list of priorities. We took this decision because we felt that this was a more efficient way of ensuring that we meet the targets set out in the EDPS Strategy.

In the case of KPI 7, we are not currently able to accurately measure the number of visitors to the EDPS website, due to a change in the cookie and tracking policy on our website ([see section 7.1.1](#)). This change is aimed at ensuring that users of our website will be able to consciously *opt-in* to having their online activity tracked on the EDPS website. It will therefore ensure that the website is as data protection friendly as possible. For this reason the results for KPI 7 are not complete.

The target for KPI 4 is readjusted yearly, in accordance with the legislative cycle.

KEY PERFORMANCE INDICATORS		RESULTS AT 31.12.2018	TARGET 2018
<b>Objective 1 - Data protection goes digital</b>			
KPI 1 Internal Indicator	Number of initiatives promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	9	9 initiatives
KPI 2 Internal & External Indicator	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8	8 initiatives
<b>Objective 2 - Forging global partnerships</b>			
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	31	10 cases
<b>Objective 3 - Opening a new chapter for EU data protection</b>			
KPI 4 External Indicator	Level of interest of stakeholders (COM, EP, Council, DPAs, etc.)	15	10 consultations
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	95%	70%
KPI 6 Internal Indicator	Rate of implementation of cases in the EDPS priority list (as regularly updated) in form of informal comments and formal opinions	N/A	N/A
<b>Enablers - Communication and management of resources</b>			
KPI 7 Composite External Indicator	Number of visits to the EDPS website	N/A	Reach 195715 (2015 results) visits
	Number of followers on the EDPS Twitter account	14,000	9407 followers (2017 results) + 10%
KPI 8 Internal Indicator	Level of Staff satisfaction	75%	75%
KPI 9 Internal Indicator	Budget implementation	93.8%	90%

Figure 1. EDPS KPI analysis table

## 3. Main Objectives for 2019

The following objectives have been selected for 2019 within the overall [Strategy for 2015-2019](#). We will report on the results in the 2019 Annual Report.

### Ensuring the correct application of Regulation 2018/1725

The [new data protection rules](#) for the EU institutions and bodies became fully applicable on 11 December 2018 (see [section 4.1.2](#)). In 2019, we will continue our campaign to ensure that both those who work for the EU institutions and those who do not are able to develop a better understanding of the requirements of the new Regulation and greater awareness of the risks associated with the processing of personal data.

Within the EU institutions, we will continue our focus on encouraging the development of a culture of [accountability](#). This involves providing [Data Protection Officers](#) (DPOs), management and EU staff members with the knowledge and tools to go beyond simple compliance, to ensure that they are also able to demonstrate this compliance.

### A new legal basis for policy and consultation activities

Regulation 2018/1725 strengthens the role of the EDPS in our policy and consultation activities. The European Commission is now explicitly required to consult the EDPS in specific cases and we must provide them with advice within eight weeks of receiving their request. The new legislation also allows for the possibility of issuing joint opinions with the European Data Protection Board (EDPB).

In 2019, we will work with the Commission and the EDPB to ensure that appropriate procedures are put in place to support these new provisions and we will review and update our internal rules and other relevant guidance documents. We will also remain at the disposal of the European Commission, European Parliament and the Council to provide formal or informal advice at any point in the decision-making process.

### Providing guidance on necessity and proportionality

In 2019, we will complete our work on providing a methodology for the EU legislator to follow when

assessing the necessity and proportionality of legislative measures with an impact on the fundamental rights to privacy and data protection. Specifically, we will develop Guidelines on proportionality, completing the work we started with the publication of our [Necessity Toolkit](#) in April 2017. In doing so, we aim to provide the EU institutions with a framework that will help them to take a proactive approach to implementing data protection safeguards into EU policy.

### Facilitating wider debate on interoperability

In our 2018 [Opinion](#) on interoperability between the EU's [large-scale IT systems](#) (see [section 4.3.4](#)) we called for wider debate on the future of these systems, their governance and on how to safeguard fundamental rights in this area. We will launch this debate in 2019, with a high-level panel on the topic at the annual Computers, Privacy and Data Protection Conference (CPDP), taking place in Brussels from 30 January-1 February 2019.

The new Regulation 2018/1725 provides for a single model of coordinated supervision for the EU's large-scale IT systems and EU bodies, offices and agencies, to be carried out by the EDPS and national supervisory authorities (see [section 4.3.2](#)). Alongside our partners in the national DPAs, we will reflect on the future of coordinated supervision over the course of 2019.

### Securing information

The new Regulation for data protection in the EU institutions introduces new concepts that emphasise the importance of information security. These include mandatory data breach notifications and the use of pseudonymisation as a recognised security measure.

To account for this, we will need to increase our capacity and competence to supervise and assess the measures taken by the EU institutions to achieve compliance. We must also be able to react quickly to notifications of data breaches and other security incidents, to ensure that any negative effect on the fundamental rights of individuals is limited. We will continue to conduct inspections focused on technological aspects, in particular those relating to large-scale IT systems (see [section 4.3.1](#)) and in the area of security and law enforcement.

## Managing the transition to Eurojust supervision

With our supervisory role at Europol now well established (see section 4.2), in 2019 the EDPS will take on the task of supervising personal data processing at another EU agency working in the field of justice and home affairs: Eurojust (see section 4.4.13).

A new legal framework for Eurojust, which includes new data protection rules specific to the agency's activities, was adopted on 6 November 2018. It provides for a supervisory role to be performed by the EDPS. To prepare for our new role, EDPS staff will organise internal and external training sessions related to Eurojust supervision, all aimed at ensuring that we are ready to take on our new role at the end of 2019.

## Implementing data protection by design and by default in the EU institutions

Under the new data protection rules, EU institutions have an obligation to implement the principles of data protection by design and by default when developing and operating data processing systems (see section 4.1.4). We will therefore increase our efforts to identify and promote practical technological solutions in 2019. This will involve regularly monitoring ICT developments in order to provide guidance and training on the technical implementation of data protection.

## Guidance on technology and data protection

In 2018, we issued Guidelines on the protection of personal data in [IT governance and management](#), [cloud computing](#) and [data breach notifications](#). In 2019, we will issue updated guidance aimed at improving accountability in IT, and provide policy advice on specific technologies or methodologies, with a special focus on security.

In order to ensure consistency with the advice and practice of other [data protection authorities](#) (DPAs), we will follow the EDPB's guidance on these topics and contribute to their work on harmonised guidance.

We will also continue to cooperate with our international partners on technology and data protection, including the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and its Working Groups and the International Working Party on Data

Protection and Telecommunications (IWGDPT, known as the Berlin Group) (see section 4.5.2).

Through carrying out inspections and investigations, we will continue our efforts to assess data protection compliance within the EU institutions. Where possible, we will endeavour to carry these out remotely, from the EDPS lab.

## Supporting the Internet Privacy Engineering Network (IPEN)

As a network of technology and privacy experts from DPAs, industry, academia and civil society, [IPEN](#) will play an important role in translating data protection principles into engineering requirements. We will support the network in intensifying its efforts to promote privacy friendly technology and privacy-aware engineering techniques. In particular, we will concentrate our efforts on translating the principle of privacy by design into engineering requirements and on facilitating an exchange between engineers and privacy experts on technical solutions for privacy issues, through workshops and presentations at public events.

The new legal obligation to apply the principle of data protection by design and by default in the design and operation of IT systems used for the processing of personal data has increased the importance of the work in this domain, in particular with respect to determining the state of the art and its development as a benchmark for supervision and enforcement activities.

## Continued cooperation with EU and international partners

With new EU legislation now fully applicable, cooperation with our data protection partners within and outside the EU is more important than ever. Cooperation with the Member State DPAs will continue on many levels and within the EDPB in particular, where our focus will be on continued active involvement with the work of the Key Provisions subgroup and as a member of the drafting team tasked with elaborating amendments to the EDPB Rules of Procedure.

Continuing our work with international organisations, we will organise a workshop in mid-2019, which will take place in Paris. Our efforts to promote a dialogue at international level with authorities, organisations and other groups from outside the EU will also remain a priority.

## Maintaining momentum for the Ethics Initiative

After the success of the [2018 International Conference of Data Protection and Privacy Commissioners](#) (see [sections 4.6.3 and 4.7](#)), our challenge now is to ensure that this momentum continues. At an event to be held as part of the Computers, Privacy and Data Protection (CPDP) Conference at the beginning of 2019, we will launch several new activities aimed at doing just this. These will include:

- a series of public conversations in the format of conference calls, web-streamed discussions or podcasts, with experts from various fields, including DPAs;

- opinion pieces from thought-leaders on the topic of digital ethics, which will be posted online;
- a new EDPS Opinion on Ethics, building on our [2015 Opinion](#) and the [Ethics Advisory Group Report](#).
- a side event on ethics which will take place during the 2019 International Conference of Data Protection and Privacy Commissioners.

Through these activities, we hope to make continued progress towards achieving an international consensus on digital ethics.

## | 4. 2018 Highlights

The new legislative framework was, once again, a significant focus of our work in 2018. Ensuring the successful launch of the European Data Protection Board (EDPB) and contributing to the work of the Board throughout the year was one aspect of this. The considerable time and effort invested in preparing the EU institutions for the [new data protection rules](#) applicable to their work was another. We also continued to push for the EU legislator to adopt the much-needed new Regulation on ePrivacy.

Our role as the data protection supervisor for the EU's police authority, Europol, is now well established. After more than a year in this role, we now have a strong working relationship with our counterparts at Europol and are making good progress in our efforts to strike the right balance between security and privacy when dealing with data processing for the purpose of law enforcement.

Finding the right balance between security and privacy is also a concern in other areas of EU policy. We responded to several new policy proposals in 2018, aimed at keeping EU borders secure. Meanwhile, we continued to work closely with EU institutions and national authorities to ensure effective and coordinated supervision of the processing of personal data in existing [border control systems](#).

However, it is not just EU border policy which has implications for data protection. In 2018 we issued Opinions on a wide range of different topics, all aimed at ensuring that the proposals put forward by the EU legislator adequately respect and protect the rights to data protection and privacy. One example of this was our [Opinion](#) on the interoperability of the EU's large-scale databases.

In our role as a data protection supervisor, we responded to complaints, carried out inspections and issued [prior check Opinions](#), in order to help the EU institutions ensure compliance with the relevant rules. We stepped up our close cooperation with [Data Protection Officers](#) (DPOs) and other EU staff members, organising meetings, visits and training sessions all aimed at preparing them for the new rules.

We continued to work closely with our data protection partners and others around the world, in our efforts to establish a more international approach to data

protection policy. As in previous years, we contributed fully to European and international discussions on data protection, collaborating with the Council of Europe on the development of a new international convention on data protection, among other things. We monitored and provided advice on international data transfers and made further progress in our work with international organisations.

Digital ethics provided another forum for international cooperation, as we increased our efforts to encourage debate on the topic around the world and across disciplines. The [2018 International Conference of Data Protection and Privacy Commissioners](#) proved a significant milestone for the [EDPS Ethics Initiative](#), launching the debate on the international stage.

Achieving our goals and living up to expectations would not be possible without the support of our Secretariat. Their activities are essential to ensuring the administrative efficiency of the EDPS and making sure that our work reaches the audience it is intended for.

As the current EDPS mandate moves into its final year, we look to 2019 as a chance to consolidate and build on our achievements, in order to ensure that we are able to meet the objectives we set ourselves in the [EDPS Strategy](#). With the importance of data protection now firmly established on the international agenda, we have no doubt that the EDPS will continue to serve as an important point of reference for all things data protection in the EU.

### 4.1 PREPARING FOR A NEW LEGISLATIVE FRAMEWORK

2018 marked the beginning of a new era in EU data protection. On 25 May 2018, the [General Data Protection Regulation](#) (GDPR) became fully applicable to all companies, organisations and institutions operating in the European Union. The new legislation also established the European Data Protection Board (EDPB), a new EU body responsible for facilitating cooperation between the EU's national [data protection authorities](#) (DPAs). The EDPS participates fully in the activities of the Board and provides its secretariat.

Two days before the launch of the GDPR, the EU legislator reached an agreement on equivalent rules for the EU institutions, bodies and agencies. This

legislation, which also defines the role and powers of the EDPS as the supervisory authority for the EU institutions, became fully applicable on 11 December 2018. In preparation for the new rules, we invested significant energy and resources in ensuring that the EU institutions were adequately prepared, providing training sessions for all levels of EU management and staff and producing relevant guidance, among other activities.

These two new Regulations, along with the Data Protection Law Enforcement Directive applicable since 6 May 2018, reinforce the EU's position as a global leader in data protection and privacy practice. They also go a long way towards helping us to achieve the strategic objective of opening a new chapter for EU data protection, set out in the [EDPS Strategy 2015-2019](#).

However, one piece of this regulatory puzzle is still missing. Only by concluding a new ePrivacy Regulation, which accurately reflects and supports the principles outlined in the GDPR, can we ensure that the fundamental rights of data protection and privacy are fully respected. In line with our Strategy commitments, we will continue to support the efforts of the EU legislator to come to an agreement on a new ePrivacy Regulation before the end of the current EU legislative period in May 2019.



#### 4.1.1 The EDPB gets to work

On 25 May 2018, the day on which the GDPR became fully applicable for all businesses and organisations operating in the EU, the EDPB started its work.

Established under the GDPR, the Board replaces the Article 29 Working Party (WP29) as the forum for cooperation between the DPAs of the 28 Member States and the EDPS. It also takes on many new tasks, aimed at ensuring the consistent application of the GDPR across the EU. In addition to this, the Board is able to issue decisions, 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. Operational from day one of the GDPR, the secretariat not only provides administrative and logistic support for the EDPB, but also carries out relevant research and analysis tasks. In addition to providing the secretariat, the EDPS is a full member of the Board and attended the five EDPB plenary meetings which took place between May and December 2018.

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

EDPS representatives attended the subgroup meetings that took place in 2018. Among a number of topics, members shared their views on the consistency and cooperation mechanisms designed to harmonise data protection practice across the EU, including the functioning of the so-called One Stop Shop mechanism. Also discussed was the performance of the Internal Market Information (IMI) System, the IT platform used to exchange information on cross-border issues, as well as the challenges and types of questions received by DPAs under the GDPR. Most DPAs reported a substantial increase in the number of complaints received since 25 May 2018.

The Board adopted 26 [Opinions](#) in 2018, establishing a list of cases in which organisations must carry out Data Protection Impact Assessments (DPIAs). These lists are an important tool in ensuring the consistent application of the GDPR across the EU. An [Opinion](#) on the new eEvidence Regulation was also adopted, as well as various other letters and documents, including Guidelines on the [territorial scope of the GDPR](#), on [GDPR certification](#), on accreditation and on [derogations for international transfers](#). On 5 December 2018, the EDPB also adopted an Opinion on the draft EU-Japan adequacy decision for international data transfers (see [section 4.5.1](#)).

In order to confront the Board's increasing workload, the number of plenary meetings is set to double in

2019. As we enter a new era in data protection practice, we look forward to continued and increasing cooperation with our fellow DPAs through the newly-established EDPB.

#### 4.1.2 The data protection Regulation for EU institutions



@EU\_EDPS

Regulation 2018/1725 on protection of natural persons w/ regard to processing of [#personaldata](#) by [#EUInstitutions](#), bodies, offices & agencies enters into force today, bringing [#dataprotection](#) rules for [#EUI](#) in line w/ standards imposed by [#GDPR](#) <https://europa.eu/!Kx84fu> [#GDPRforEUI](#)

#### Regulation 2018/1725

While the GDPR applies to all companies and organisations that process personal data within the EU, it does not apply to the EU institutions, which must adhere to separate rules.

On 23 May 2018, two days before the GDPR became fully applicable, representatives from the European Parliament and the Council agreed on a new Regulation on the handling of personal data by EU institutions and other EU bodies. The text was adopted at the European Parliament Plenary Session on 13 September 2018 and in the Council a month later. On 23 October 2018, it was signed by the Presidents of the European Parliament and the Council of the EU. Published in the Official Journal of the EU as [Regulation 2018/1725](#) on 21 November 2018, the new rules became fully applicable on 11 December 2018.

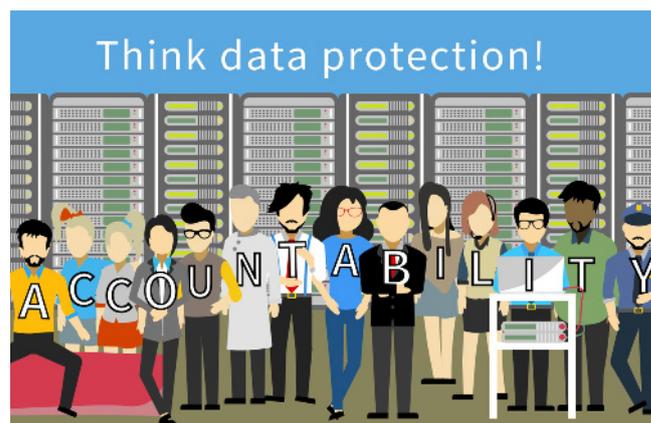
It is vital that, when dealing with the EU institutions, all EU employees and citizens are able to enjoy the same strengthened rights as they would under the GDPR. The new Regulation, therefore, brings the data protection rules for the EU institutions, previously set out in [Regulation 45/2001](#), in line with the high standards provided for in the GDPR.

Regulation 2018/1725 also includes a specific chapter on the processing of operational personal data by EU agencies working in the field of law enforcement and judicial cooperation in criminal matters, such as Eurojust. These rules are aligned with those set out in the Law Enforcement Directive which, like the GDPR, became applicable in May 2018. The agencies operating in this area have the option to develop more detailed rules on the subject and include them in their founding acts. This will allow the agencies to account for any particularities in the way they operate.

For now, the processing of operational personal data by Europol and the European Public Prosecutor's Office remains outside the scope of these new rules, with the European Commission set to review the situation by 2022.

#### Coordinating the transition to the new Regulation

In anticipation of the new rules, we worked closely with [Data Protection Officers](#) (DPOs) and other representatives from all EU institutions, bodies and agencies throughout 2017 and 2018 to ensure they were prepared. These activities included interactive workshops organised as part of our twice-yearly meetings with DPOs ([see section 4.4.1](#)), as well as targeted visits, training sessions and conferences. Our aim was to ensure that all EU staff involved in the processing of personal data, regardless of their place in the EU hierarchy, were aware of the new rules and what they entail.



Our awareness-raising campaign intensified in 2018, in order to provide the EU institutions with the necessary knowledge and tools to apply the new rules with ease. The campaign put particular emphasis on the importance of [accountability](#), the idea that EU institutions not only comply with the new rules, but that they are also able to demonstrate this compliance. We asked top management to set the tone, by integrating data

protection into risk management plans and ensuring that data protection is ingrained within the culture of their respective institution.

To help them with this, we published updated and new [guidance documents](#) on topics such as accountability, risk assessment and Data Protection Impact Assessments (DPIAs), data breach notifications and transparency and information obligations, as well as an updated position paper on the role of the DPO (see [section 4.4.1](#)). This guidance was reinforced through a programme of visits, training sessions and conferences, including a [visit to EU institutions and bodies in Luxembourg](#) by Assistant Supervisor Wojciech Wiewiórowski, a [training session](#) for staff at the EU agencies in Athens, an exchange with [communication officers from the EU institutions](#) and a [training session](#) for staff working for the EU agencies in Italy, as well as numerous bilateral and other meetings with top management in the EU institutions. (see [figure 2](#)).

As an EU institution, we are also subject to the new rules. To help us prepare, we set up an Internal Task Force on the Transition to the New Regulation. We wanted to ensure that we were able to lead by example and act as an accountable [data controller](#), while also providing assistance to other EU institutions.

We look forward to working in close cooperation with the EU institutions in this new era of data protection practice, in order to ensure that they continue to lead by example in the protection of personal data across the EU and globally.

#### 4.1.3 ePrivacy: completing the EU's data protection framework



While the GDPR regulates data protection, it does not apply to the privacy of communications. Further

legislation is required, in the form of a Regulation on ePrivacy, to provide for comprehensive data protection within the EU and ensure legal certainty and a level playing field for market operators.

The current ePrivacy Directive was last updated in 2009. The proposed revision of these rules was presented by the European Commission on 10 January 2017. It would replace the Directive with a new ePrivacy Regulation, aligning the rules for electronic communications services with the standards set out in the GDPR.

Under the current rules, traditional electronic communications providers are subject to clear limitations on the way they use personal data. Companies classified as *information society services*, on the other hand, have flourished by exploiting loopholes in this legal framework. While traditional e-communications providers must seek consent for using communications data, information society services are not bound by the same obligations. There is, therefore, a clear and urgent need to close the loopholes in the current legislation and strengthen the protection of privacy and the security of online communications.

In October 2017, the European Parliament adopted a report and draft resolution on the proposed ePrivacy Regulation. We welcomed this as a positive attempt to strike a balance between the various interests at stake. Making progress in the Council, however, has been more challenging.

The scope for negotiation on many points of the proposal is limited, as it would involve compromising on the key principles of communications privacy. For example, when applied to the most sensitive types of personal data, proposed clauses allowing for the *further processing of metadata for compatible purposes* would likely widen the existing legal loophole and present service providers with a way of circumventing the high level of protection provided under the GDPR.

It is crucial that the new ePrivacy Regulation does not lower the level of protection provided by the GDPR. On the contrary, given the importance of ensuring the confidentiality of communications and the particularly sensitive nature of the metadata it involves, what is urgently needed is legislation that provides a higher level of protection. From a data protection and privacy perspective, we strongly believe that there is no excuse for failing to come to an agreement on the ePrivacy Regulation before the end of the current legislative period. Not doing so will only increase the risk of an uncertain outcome.



# EDPS Training

## 2018



### Brussels - 31 January

We kicked off the year by staying close to home, providing a training course for the European Ombudsman in Brussels (also available to Ombudsman employees in Strasbourg via video link). The course was attended by Heads of Units and Sectors, as well as other relevant staff members.

### Brussels - 16 February (and more)

We staged a two-hour training for EU managers at the European Union School of Administrators (EUSA). This was no one off - we would return to EUSA on six further occasions throughout the year. Thanks to our trainings, EUSA staff are now in a stronger position to negotiate the new Regulation 2018/1725.

### Lisbon - 25 May

On 25 May, we celebrated the entry into force of the GDPR with colleagues from the European Maritime Safety Agency (EMSA) and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) by giving a training event preparing them for the transition to the new Regulation.

### Brussels - 7 June

As summer entered into full swing, we ventured over to Avenue de Beaulieu in Brussels to provide training on new data protection commitments for employees working in DG CLIMA, DG MOVE and other interested colleagues.

### Maastricht - 26 June

On 26th June, and again on 3rd December, the Head of Inspections at the EDPS travelled to Maastricht to give a presentation to participants of EIPA's Data Protection Certification. The two-hour talk was entitled 'supervising data protection compliance: the role of data protection authorities'.

### Luxembourg - 30-31 January

Other EDPS colleagues ventured slightly further afield, providing a two-day training for those working in EU institutions based in Luxembourg. Over 200 guests participated. Whilst there, we delivered a high-level management training session for representatives from the European Parliament, the Commission, CJEU, ECA, EIB, CDT, EIF and CHAFAEA

### Athens - 1-2 March

This two-day training event, provided for staff working at ENISA and CEDEFOP, was a handy opportunity to reaffirm current data protection obligations and introduce the new obligations under the revised Regulation. We also launched a case study on events management which proved so useful that it was re-used at other training sessions throughout the year.

### Brussels - 29 May

Just four days after the General Data Protection Regulation (GDPR) entered into force, the EDPS welcomed 23 recently appointed Data Protection Officers (DPOs) and assistant DPOs from the EU institutions and bodies to a training course on the effective protection of personal data in their new role. A second, similar DPO training event would take place on 10 December.

### Brussels - 14 June

We presented a webinar to the Publications Office of the EU and other EU staff working in publications, communications, social media and web teams. Our work didn't stop there, however. On the same day, we ran a training event for the European Union External Action Service (EEAS).





### Luxembourg - 1-2 October

Invited by the Court of Justice of the EU (CJEU), we returned to Luxembourg to give a training on the new Regulation. Over 400 guests were in attendance, hailing from a number of different EU institutions.

### Stockholm - 18 September

We provided a training session at the annual meeting of the network of web managers from the EU agencies and bodies. It proved a fantastic opportunity to interact directly with EU communication officers on data protection matters.

### Brussels - 7 November

We ran a data protection training event for DG FISMA, the Commission department responsible for EU policy on banking and finance, covering data protection basics, data subject rights and a case study on event management.

### Brussels - 20 November

Just one day before Regulation (EU) 2018/1725 was published, the final training of 2018 was put on for staff of the EFTA Surveillance Authority.

### Paris - 26 November

As we approached the end of the calendar year, the EDPS made a trip to Paris for a Compliance Visit to the European Union Institute for Security Studies. With Assistant Supervisor Wojciech Wiewiórowski also present, the S&E team gave a training on the new Regulation.



### Brussels - 23 October

The European Commission and the national competition authorities in all EU Member States cooperate with each other through the European Competition Network (ECN). In October, we paid DG COMP a visit to guide the ECN on data protection matters in investigations and inspections.

### Turin - 20-21 September

At the request of the European Training Foundation (ETF), we ran through data protection case studies with a wide range of colleagues, including participants from the ETF, the European Food Safety Authority (EFSA), the Joint Research Centre (JRC) and the European University Institute (EUI).

### Frankfurt - 12 November

We were Germany-bound in mid-November to provide a training event on data-protection aspects of banking supervision in cooperation with the Data Protection Officer of the European Central Bank (ECB), the private sector (Union Investment) for ECB staff, and staff of the European Insurance and Occupational Pensions Authority (EIOPA) in Frankfurt.

### Brussels - 21 November

21st November saw the EDPS give a presentation to the Committee for Civil Aviation Security at DG MOVE.

### Brussels - 3 December

The EDPS ended the year's training sessions in the same place in which we started, at home in Brussels. We provided training to DG COMM and other European Commission representations on how the new Regulation would affect their events.

Figure 2. EDPS training programme 2018



#### 4.1.4 Privacy by Design: technology that serves the people

The public debate on the misuse of personal data for tracking and profiling purposes and the role of technology in our society intensified over the course of 2018. One element of the debate is whether companies should be able to take advantage of technology exclusively as a means to increase profits, or whether they should also be obliged to use it to further the interests of individuals and the common good.

The GDPR introduced the principles of data protection by design and by default as essential obligations in ensuring accountability. Those responsible for collecting and processing personal data must put in place appropriate technical and organisational methods to ensure and demonstrate data protection compliance. Both principles have the potential to help establish the human perspective as the main driver for technological development. Data protection by design involves planning for the integration of personal data protection into new technological systems and processes from the design stage of a project and throughout its whole lifecycle, while data protection by default involves integrating privacy protection into all technological services and products as a default setting.

On 31 May 2018, just a few days after the GDPR became fully applicable, we published a [Preliminary Opinion on Privacy by Design](#). The Opinion aimed to build on our work with the [Internet Privacy Engineering Network \(IPEN\)](#) (see section 4.4.16) and on the [EDPS Ethics Initiative](#) (see section 4.6), to encourage dialogue between policymakers, regulators, industry, academia and civil society on how new technologies can be designed to benefit the individual and society. We look forward to further debate on this issue in our attempts to establish a common approach to technological development which puts human dignity first.

## 4.2 SUPERVISING EUROPOL

Europol is the EU body responsible for supporting Member State law enforcement authorities in the fight against serious international crime and terrorism. On 1 May 2017, the EDPS assumed responsibility for supervising the processing of personal data at Europol.

The [Europol Regulation](#) tasks the EDPS with supervising the processing of personal data relating to Europol's operational activities. We are also responsible for supervising the processing of personal data relating to Europol's administrative activities, including personal data relating to Europol staff. However, this supervisory task is subject to the rules now set out in the new [Regulation 2018/1725](#), which replaces [Regulation 45/2001](#).

One of the main challenges we face in this role is to ensure that Europol strikes the right balance between security and privacy when dealing with data processing for the purpose of law enforcement. A secure and open Europe requires improved operational effectiveness in the fight against cross-border crime, but it also requires a commitment to protecting the fundamental rights and freedoms of individuals.

### 4.2.1 Continuous cooperation with Europol's data protection unit

Under the Europol Regulation, Europol must appoint a [Data Protection Officer \(DPO\)](#), who is to act independently in the performance of all duties. Through close cooperation with Europol's DPO and Data Protection Function (DPF) unit, we are better equipped to monitor Europol's compliance with the Regulation and to provide advice to the DPF team when they need it.

We aim to facilitate and reinforce our cooperation by holding regular meetings with the DPF and other relevant operational staff. These meetings, which usually take place on a bimonthly basis, are an opportunity to discuss any new projects or data processing procedures planned by Europol, as well as other pending issues.

Over the past year, the EDPS and the DPF have met four times in The Hague, on 8 February, 24 April, 9 July and 16 October 2018. We also met with the DPF and other Europol staff members in Brussels on 25 September 2018. These meetings help us to anticipate specific issues relating to data processing activities at Europol and to define and plan for future activities, such as inspections or inquiries. Three EDPS staff members also participated in the European Data

Protection Experts Network (EDEN) conference, which took place on 22-23 November 2018 (see section 4.2.7).



#### 4.2.2 Supervising operational analysis projects

The Europol Regulation allows for the processing of personal data to support what is known as operational analysis. However, it specifies that these criminal investigations and criminal intelligence operations, which are carried out by Member State law enforcement authorities, must be performed as part of an operational analysis project.

Each operational analysis project relates to a particular type of crime, such as child pornography, cybercrime, drug trafficking, organised criminal groups, property crimes or terrorism. For each project, Europol is required to define and inform the EDPS about:

- the specific purpose of the project;
- the categories of data involved and the individuals it concerns;
- the participants, which could be Member States, non-EU countries or organisations;
- the length of time that the data will be stored;
- the conditions for access to the data concerned and for any proposed transfer of this data.

At the end of 2018, Europol had a portfolio of 30 operational analysis projects. We did not receive formal notification of any new projects in 2018, although we were notified of smaller amendments to existing projects and were consulted on the envisaged amendments prior to the actual modification of the portfolio. All analysis projects are listed and described on the [Europol website](#).

#### 4.2.3 Inspecting Europol

On 8 May 2018, we issued a report on our first Europol inspection, carried out in December 2017. As with our other inspections (see section 4.4.6), the results were not shared publicly, but the report was shared with the national [data protection authorities](#) (DPAs) through the secretariat of the Europol Cooperation Board (see section 4.2.6). We outlined a number of recommendations for improvement and we will continue to work with Europol to ensure they put our recommendations into practice.

We carried out a second inspection from 22-25 May 2018. Three experts from the DPAs of France, Greece and Italy joined the inspection as part of the EDPS team. The Member States are Europol's main information providers so, as well as benefitting from their expertise, the participation of national experts in the inspection process helps to raise awareness of any problems arising at Europol level which might have originated at national level. This could include problems with data quality or insufficient justification for the processing of sensitive data, for example. They can then consider how to tackle these problems in their supervisory activities at national level.

The legal part of the inspection focused on four topics, the first two of which were particularly high-profile:

1. **The processing of data as part of Europol's operational analysis project, *Travellers*:** This concerns the personal data of individuals who travel to and from conflict zones, Syria in particular. It encompasses those known as foreign terrorist fighters and their families, including children.
2. **The processing of data on migrants arriving at hotspots in Greece and Italy:** The European Border and Coast Guard Agency (Frontex) interviews migrants upon their arrival in these countries. If an individual is believed to present a possible security risk, Member States can turn to Europol *guest officers*, also situated in the hotspots, to run checks on them.
3. **The processing of data relating to individuals under the age of 18 in all operational analysis projects, particularly in cases when such individuals are labelled as suspects:** Under the Europol Regulation, Europol is only permitted to process the personal data of under 18s if doing so is strictly necessary and proportionate to the aim of preventing or combatting crime under Europol's mandate.
4. **The processing of data in the Europol Information System:** This is Europol's database of

suspects, convicted persons and potential future criminals. In particular, we focused on how this database is updated by Member States and Europol on behalf of non-EU countries.

The technical element of the inspection looked to build on the activities carried out as part of our first inspection. We focused on three areas in particular:

1. Europol's information security management procedures;
2. user log management;
3. the validation process for new tools and IT systems.

We issued our inspection report on 19 December 2018. We will follow-up with Europol on our specific recommendations throughout the coming year.

In 2018, we also carried out remote inspections of two Europol websites as part of our follow-up exercise on the protection of personal data processed by EU institution websites (see section 4.4.7).

#### 4.2.4 Advising Europol

The EDPS advises Europol on all matters concerning data protection, either on our own initiative or in response to a consultation.

##### Prior Consultations

Europol must submit a prior consultation request to the EDPS for every new data processing activity they plan to carry out which involves the processing of sensitive data or which might present a specific risk to individuals. Based on Europol's submission, we analyse how far the proposed processing operation complies with the Europol Regulation and all other relevant data protection principles and rules. We then provide Europol with recommendations which they must implement in order to ensure compliance.

In 2018, we issued three Opinions. These all related to prior consultations received at the end of 2017. The Opinions concerned the following technical tools:

- **QUEST (Querying Europol Systems):** An automatic interface used to facilitate [cross-checking](#) of data in the national databases and Europol's suspect database. Through its simplified search mechanism, QUEST provides Member States with new search capabilities. This enables authorised Member State police officers to carry out simultaneous searches of the Europol information system and other national and international databases from their own

working environments, using their national databases.

- **ETS (European Tracking Solution):** A tool that enables specialist units, based predominantly in the Member States, to exchange geo-location data in near real-time. It is used to track and trace objects and individuals.
- **IRMa (Internet Referral Management application):** A software tool used by Europol's Internal Referral Unit (IRU) to help automate the *referral process*, the process of identifying online terrorist content and notifying online service providers of the need to remove it. Europol developed this tool and would like to provide it to Member States, to use for the same purpose.

Given that these Opinions refer to the use of tools by national law enforcement authorities, which may involve supervision by the respective national supervisory authorities, the EDPS shared the Opinions with them.

In 2018, we received one additional prior consultation on SIENA 4.0, the updated version of Europol's secure message exchange system. It is used to manage the exchange of operational and strategic crime-related information among Member States, Europol and Europol's other partners. We will issue feedback on this prior consultation in 2019.

##### Consultations and inquiries

We issued guidance and conducted own initiative inquiries on a number of issues in 2018. One of these cases was a consultation relating to the Internet Corporation for Assigned Names and Numbers (ICANN). Our [Opinion](#) addressed whether Europol should serve as an accrediting body for law enforcement agencies (LEAs) looking to access personal data in the WHOIS database, the Internet's Domain Name System which is managed by ICANN.

Before the [General Data Protection Regulation](#) (GDPR) came into effect on 25 May 2018, the personal data of anyone registering a new domain name was publicly displayed on the internet, through the WHOIS service. This included names, email addresses, phone numbers and other forms of identifying information.

However, in order to adhere to the requirements of the GDPR, this previously public information is now being redacted. This has created problems for LEAs, who no longer have such easy access to the personal data of domain name registrants, and are now required to conclude formal legal procedures in order to access the relevant information.

Our Opinion concluded that Europol could act as a *law enforcement accreditor*. This would involve providing assurances to registries and registrars that any EU LEA seeking to access WHOIS records is indeed a legitimate authority, so long as the activity concerned falls within Europol's mandate, as a support authority for the Member States.

In a separate case, we provided guidance on the transfer of personal data from the European Border and Coast Guard Agency (Frontex) to Europol. Frontex is involved in monitoring migratory flows and carrying out risk analysis on integrated border management, including internal security or security at the EU's external borders. Our guidance concerned any data transfers from Frontex to Europol in relation to these activities.

In addition to this, we conducted an inquiry on data processed in the context of the 'Crime Information Cell' (CIC), a pilot project activated on board EUNAVFOR MED operation *Sophia*, operating in the Central Mediterranean Sea. Following a decision of the Council of the EU of 14 June 2018, specialised personnel from Europol and Frontex have embarked on board Flagship EUNAVFOR MED. The goal is to enhance the exchange of information between Common Security and Defence Policy (CSDP) and Justice and Home Affairs (JHA) actors on criminal activity in the Central Mediterranean and to disrupt criminal networks in the area, notably those involved in migrant smuggling and human trafficking.

We also advised Europol on possible developments relating to FIU.net. This is the decentralised information network which supports the EU's Financial Intelligence Units (FIUs) in their fight against money laundering and the financing of terrorism. It is operated by Europol.



#### 4.2.5 Dealing with complaints

The EDPS is also responsible for hearing and investigating complaints from people who believe that

Europol has mishandled their personal data. Europol relies on national law enforcement authorities to provide them with the majority of the personal data it processes. As these national authorities are supervised by their national DPA, we work in consultation with the relevant national DPAs to investigate all admissible complaints and adopt decisions.

Of the two complaints received in 2017, only one was considered admissible. It related to a claim that Europol denied access to personal data requested by the individual concerned. We investigated the complaint, examining Europol's file on the decision and taking into account the observations of the national DPA involved. Our conclusion, issued in 2018, was that Europol's decision to refuse access to personal data was lawful in this case.

In 2018, we received just one complaint, which was deemed inadmissible.

#### 4.2.6 Meeting with the Cooperation Board

Just as the EDPS is responsible for supervising the processing of personal data by Europol, the national DPAs are responsible for overseeing the processing of personal data by their respective national law enforcement authorities. As most of the data processed by Europol comes from the national law enforcement authorities, it is essential that we are able to cooperate effectively with the national DPAs.

In addition to activities such as joint supervision, much of this cooperation takes place in meetings of the Cooperation Board, for which the EDPS provides the secretariat. The Board has an advisory function and provides a forum to discuss common issues and develop guidelines and best practice.

Composed of representatives from the relevant national DPAs and the EDPS, the Board meets at least twice a year. In 2018, these meetings took place on 30 May and 3 October.

The first meeting provided an opportunity for us to share information on the supervisory activities that had taken place since our previous meeting on 16 November 2017. This included our first Europol inspection. It was also a chance to discuss the work programme of the Board for the next two years.

Assistant Supervisor Wojciech Wiewiórowski opened our second meeting. In his speech he stressed that fruitful cooperation between the EDPS and DPAs depends on trust and reciprocity. Only in such an environment can the Board be successful in protecting citizens' rights.

We then focused on Europol activities that have an effect at national level. For example, Europol provides tools which facilitate the exchange of information between national law enforcement authorities and the national DPAs are responsible for supervising their use at national level. In this respect, discussions took place on the use of ETS by national law enforcement authorities and on possible developments of FIU.net (see section 4.2.4).

An update of a leaflet aimed at helping individuals to exercise their data protection rights in relation to Europol and a handbook for national law enforcement authorities on how to send data to Europol were also discussed.

We look forward to strengthening our cooperation with the Board as we work towards achieving the joint aim of a secure and open Europe.

#### 4.2.7 Setting the tone at management level

On 8 March 2018, Catherine De Bolle, former Commissioner General of the Belgian Federal Police, was appointed as the new Executive Director of Europol. Accompanied by the Europol DPO and two members of her Cabinet, she visited the EDPS on 16 July 2018 to meet with EDPS Giovanni Buttarelli. This meeting was an excellent opportunity for both parties to get to know one another and establish the foundations for effective cooperation based on mutual trust.

Their exchange of views was both frank and constructive. The new Executive Director showed a good understanding of data protection issues in general and an even better knowledge of the main issues that Europol and the EDPS still need to address. Management sets the tone for cooperation throughout the whole organisation, so we look forward to continued and constructive cooperation at this level over the coming months and years.

In the spirit of leading by example through effective cooperation, on 22 November 2018, Assistant Supervisor Wojciech Wiewiórowski gave the keynote speech at a conference on Freedom and Security, jointly organised by the Europol Data Protection Experts Network (EDEN) and the Academy of European Law (ERA). He recalled the message outlined by former Europol Executive Director Rob Wainwright in his Data Protection Day 2018 [blogpost](#), calling for tailored data protection rules for law enforcement. He also stressed that increased security can be achieved without restricting data protection rights. Through their continued

and constructive cooperation, the EDPS and Europol are ideally placed to demonstrate this.



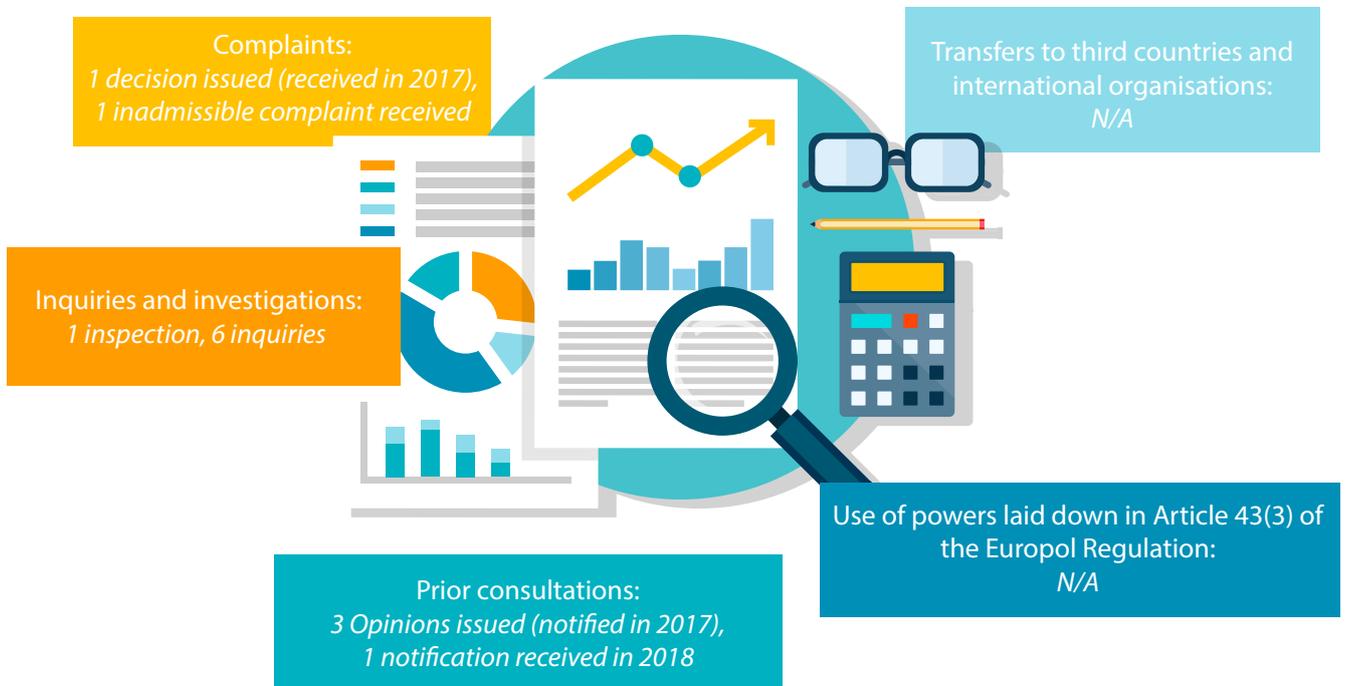
#### 4.2.8 The Joint Parliamentary Scrutiny Group

The Joint Parliamentary Scrutiny Group (JPSG) is a parliamentary supervisory body made up of more than 120 representatives from the European Parliament and national Parliaments. Its job is to hold Europol accountable for its activities. The EDPS must support the JPSG in this role.

At least once a year, the JPSG organises a meeting with the EDPS to discuss Europol compliance with data protection rules and principles. In 2018, two meetings of the JPSG took place and the EDPS was invited to attend both. These took place in Sofia, Bulgaria on 19 March 2018 and in Brussels on 25 September 2018.

The meetings are an opportunity for us to provide the JPSG with an overview of EDPS supervisory activities, as well as to discuss more specific issues. At the Sofia meeting, for example, we addressed a series of recommendations relating to the exchange of personal data between Europol and eight different Middle Eastern and African countries. These recommendations were issued by the Commission in December 2017 and advised the Council of the EU to begin negotiations for international agreements with the eight countries on the exchange of data. The EDPS published an [Opinion](#) on these recommendations just before the JPSG meeting on 14 March 2018 (see section 4.3.4).

## EDPS Supervision of Europol in 2018: the statistics



At the second meeting, we focused specifically on Europol's reliance on cooperation to perform its role, the implications of this for data protection matters and on how we are working with Europol to address such implications. Europol's partners are varied, including international partners, EU partners such as Frontex and partners at national level.

We look forward to cooperating further with the JPSG during the course of 2019.

### 4.3 SECURITY AND EU BORDERS

As we set out in the [EDPS Strategy](#), we are committed to facilitating responsible and informed policymaking within the EU and to promoting a mature conversation on security and privacy as part of our efforts to open a new chapter in EU data protection.

In recent years, the EU legislator has put forward a wide range of policy proposals aimed at increasing EU security and improving border management. Terrorist attacks, the migration crisis and the development of increasingly sophisticated technology are the main drivers behind these proposals, all of

which aim to ensure that EU processes and policies remain up to the task of ensuring safe and secure EU borders.

We fully support these efforts and recognise the pressing need for EU policy to adapt to new realities. However, increased security must not come at the expense of the fundamental rights guaranteed in the [EU Charter](#).

In line with the commitments identified in our Strategy, we seek to provide the legislator with appropriate legal advice, guidance and recommendations to ensure that policymakers are able to make informed decisions on EU border policy. Furthermore, we aim to support the legislator by working in close cooperation with our fellow [EU data protection authorities](#) (DPAs) to ensure that the tools used to implement EU border policy continue to function to the highest standards of EU data protection law.

#### 4.3.1 Effective supervision of large-scale IT systems

The European Union operates several [large-scale IT databases](#). These are used to support EU policies on asylum, border management, police cooperation and

migration. Through the databases, national authorities, as well as some EU bodies, are able to exchange information relating to borders, migration, customs and police investigations.

The EDPS is responsible for supervising the processing of personal data in the central units of the databases, the majority of which are hosted by the EU's Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA). The national DPAs are responsible for supervising how national authorities use these systems. The division of tasks between EU DPAs and the EDPS mirrors the division of tasks between the central unit managing the system and the national authorities using it. The relevant supervisory authority therefore depends on who processes the data.

One of our supervisory responsibilities is to carry out periodic inspections of the central databases. These inspections focus on the security and management of the systems, while the national authorities are responsible for ensuring the accuracy of the information entered into them. Through carrying out inspections, we are able to monitor data protection compliance, but also to work directly with eu-LISA to improve [accountability](#) in the management of these databases.

In 2018, we carried out on-site inspections of the [Schengen Information System](#) (SIS) and the [Visa Information System](#) (VIS). We will share our report and recommendations with eu-LISA, the European Parliament, the Council, the European Commission, and national DPAs in 2019 and follow up with them accordingly.

### 4.3.2 Coordinated supervision of large-scale IT systems

Just as the EDPS is responsible for supervising the central units of the EU's large-scale IT databases, the national DPAs are responsible for supervising how their respective national authorities use these databases. In order to ensure the consistency of supervision efforts on both levels, all supervisory authorities involved, including the EDPS, cooperate through [Supervision Coordination Groups](#) (SCGs). Each of these groups is dedicated to a specific EU database.

Made up of representatives from the national DPAs and the EDPS, the SCGs meet regularly to ensure coordinated end-to-end supervision of all the databases. As the supervisory authority for the central units, the EDPS participates as a full member of these groups. We also provide the secretariat for the

groups, working under the authority of their respective Chairs.

As in past years, the groups met twice in 2018. The SCGs for [Eurodac](#), SIS and VIS met in June and November, while the SCG for the [Customs Information System](#) (CIS) met in May and October. The results of these meetings are published on their [respective webpages](#) on the EDPS website. The meetings continue to provide a valuable forum for cooperation between the Member State DPAs and the EDPS, while also respecting the role and competences of each.

The new data protection rules for the EU institutions and bodies provide for a single model of coordinated supervision of both large-scale IT systems and EU agencies and bodies, within the European Data Protection Board (EDPB). The EDPB has therefore launched an initiative to reflect on how to organise this coordinated supervision within the EDPB framework.

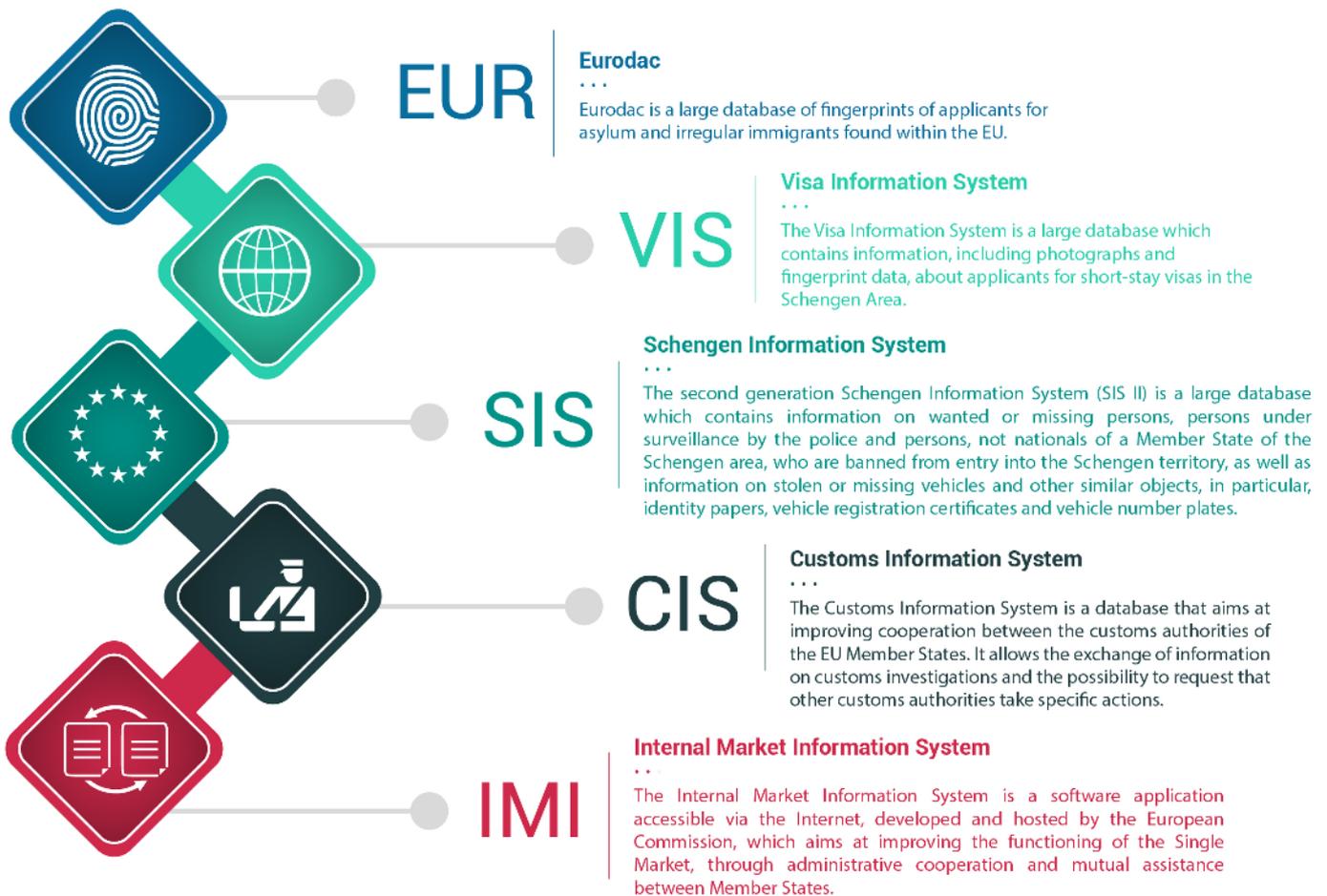
The SCGs will meet again in 2019 as part of our ongoing commitment to ensuring effective, efficient, coordinated and consistent supervision of these important databases.

### 4.3.3 Observing Schengen

The establishment of the Schengen area has made travelling between many EU countries a much easier and more enjoyable experience for EU citizens and others. However, the success of this initiative depends on a collaborative effort from all states involved.

Among the measures designed to ensure that all relevant Member States adequately implement Schengen rules are [regular peer review exercises](#). Known as Schengen evaluations (SCHEVAL), these peer reviews are organised by the European Commission and carried out by experts from the Member States. The EDPS often participates as an observer in the data protection part of the evaluation.

With our experience supervising the central units of the SIS and VIS ([see section 4.3.1](#)), the EDPS is able to offer a different and complementary perspective on the SCHEVAL process. This is of clear added value in the supervision, enforcement and promotion of data protection in this highly sensitive area. Our input is also appreciated on a linguistic level, as the international composition of our institution means that the EDPS staff members taking part in the evaluation often speak the language of the country under evaluation.



The data protection aspect of the evaluation involves assessing the competent authorities' compliance with data protection rules, including the security of the SIS and VIS databases; the independence, role and powers of the national data protection authority; public awareness of Schengen; and international cooperation. Over the course of a year, we usually take part in three SCHEVALs. In 2018 we acted as an observer for the evaluations of Switzerland, Latvia and Finland.

#### 4.3.4 Protecting fundamental rights in the area of freedom, security and justice

##### Biometric ID cards

On 10 August 2018, we issued an [Opinion](#) on the Commission's Proposal for a Regulation aimed at strengthening the security of identity cards and other documents issued to EU citizens and their families. This would involve improving the security features of EU citizens' identity cards and the residence cards of non-EU family members.

 @EU\_EDPS

#EDPS reiterates the importance of #dataprotection key principles when strengthening the security of identity cards of EU citizens. #Necessity & #Proportionality are to be respected when data is processed, especially #biometric data @EP\_Justice <http://europa.eu/!Gf93pT>

The proposal would have an impact on up to 370 million EU citizens, potentially subjecting 85% of the EU population to mandatory fingerprinting requirements. Taking into account this wide scope and the sensitive

nature of the data involved, we identified the vital need for the Commission to clearly demonstrate the necessity of the measures proposed. For example, the stated purposes for processing two separate types of biometric data, namely facial images and fingerprints, could be achieved using a less intrusive approach, and therefore fail to demonstrate necessity. We also cited the need to establish explicit safeguards to ensure that the implementation of the proposal at national level would not lead to the creation of national fingerprint databases.

While the storage of fingerprint images does enhance interoperability (see section 4.3.4), it also increases the amount of biometric data that is processed. This increases the risk of impersonation in the case of a personal data breach. Accordingly, we recommended significantly limiting the fingerprint data stored in the chip of residence documents, to include only a subset of the characteristics extracted from the fingerprint image.

Finally, the EDPS advocated setting the minimum age limit for collecting children's fingerprints to 14 years old, in line with the approach taken in other instruments of EU law.



 @EU\_EDPS

#EDPS calls for wider debate on the future of information sharing in the #EU. Read the EDPS opinion on the #interoperability between the EU large-scale information systems <http://europa.eu/!Rv88rR> and the press release <http://europa.eu/!uW44UM>

#### Wider debate needed on the future of information sharing in the EU

In order to address challenges relating to security and border management, the EU needs to adopt a smarter approach to information sharing. Interoperability could prove a useful tool, but it is also likely to have profound legal and societal consequences, as outlined in our [reflection paper](#) on the topic in November 2017.

On 16 April 2018 we followed up our reflection paper with an [Opinion](#) on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems. Interoperability is the process of enabling these large-scale EU databases to communicate and exchange information. It could help public authorities to manage issues relating to migration, asylum and security by facilitating the exchange of data held within the databases.

The proposals provide for the possibility to use the systems more extensively, beyond the specific objectives for which they were established. In particular, the data stored in the different systems would be gathered in order to combat identity fraud, but also to facilitate and allow for identity checks within Member State territory. They would also streamline law enforcement access to databases that do not contain law enforcement information. Of particular concern is the creation of a centralised database containing information about millions of non-EU citizens, including biometric data. The scale of the database and the nature of the data to be stored within it mean that a data breach could harm a very large number of people.

While law enforcement authorities need access to the best possible tools to fight terrorism and other serious crime, allowing law enforcement authorities to routinely access information not originally collected for law enforcement purposes has significant implications for the protection of fundamental rights. It is therefore essential that strict and appropriate legal, technical and organisational safeguards are built in to all EU databases, and that particular attention is given to defining their purpose and conditions of use.

Given the uncertain implications of this proposal for data protection and other fundamental rights and freedoms, we called for wider debate on the issue before any further steps are taken towards implementation.



### **Information exchange between Europol and non-EU countries in the fight against terrorism and serious crime**

The European Commission adopted eight recommendations on 20 December 2017. In these recommendations, they asked the Council of the EU for authorisation to start negotiations with Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey to conclude international agreements on the exchange of data between Europol and these eight non-EU countries.

The rules for the transfer of data from Europol to non-EU countries are outlined in the Europol Regulation. According to these rules, international agreements negotiated and concluded by the Commission would provide the required legal basis for the exchange of personal data between Europol and the authorities of these eight countries, with the aim of fighting serious crime and terrorism.

The EDPS issued an [Opinion](#) on the Commission's recommendations on 14 March 2018. We stressed that any international agreements relating to the exchange of data between Europol and non-EU countries must strike a fair balance between the need to fight serious crime and terrorism and the need to protect personal data and other fundamental rights. Each agreement must also outline the specific conditions under which Europol can transfer personal data to the country concerned, recognising that these conditions will be different for each country.

We provided some general recommendations aimed at ensuring that the negotiated agreements include the appropriate safeguards required by the Europol Regulation, but we mainly focused on the Annexes to the Commission's recommendations. These set out the mandates and directives the Council should give to the Commission in order to negotiate each agreement. As they include all data protection requirements with which the international agreements should comply, we provided recommendations on how to ensure that these requirements were comprehensive in scope.

### **Simplifying judicial cooperation on family matters**

The Brussels IIa Regulation is a Council Regulation on jurisdiction. It concerns the recognition and enforcement of decisions in matrimonial matters and matters of parental responsibility, including international child abduction. The Council formally requested an EDPS [Opinion](#) on a Proposal for a recast of the Regulation, which we published on 15 February 2018. We then presented this to the Council on 1 March 2018.

The recast of the Brussels IIa regulation establishes uniform jurisdiction on rules for divorce, separation and annulment of marriage, as well as for disputes about parental responsibility in cross-border situations. Its main objective is to remove the remaining obstacles to the *free movement* of judicial decisions, in line with the principle of mutual recognition, and to better protect children's interests by simplifying procedures and improving efficiency. The new rules also aim to avoid the creation of a new EU IT database, by improving cooperation between the central authorities involved in exchanging information within and across the Member States.

In our Opinion we provided specific recommendations to ensure that any processing of personal data is done lawfully and that suitable and specific safeguards are put in place to protect the fundamental rights and interests of the individuals concerned. We also recommended that clauses explaining the specific purposes for which data can be processed, and the individuals this concerns, be inserted into the text, in addition to explicit references to the need to respect the principles of data quality and minimisation.

To ensure that data is processed consistently and fairly across the EU, we reiterated the need to specify that any reference to the national law of a Member State should not lead to increased limitations on an individual's right to information at national level. We also recommended establishing a principle in the Regulation to provide individuals with the right to access any information transmitted to the requesting authority of a Member State. To deal with cases where restrictions on an individual's access and rectification rights are considered necessary, we expressed the need for a specific provision outlining the scope of these restrictions.

## **4.4. ON THE GROUND**

The EDPS is entrusted with ensuring that the EU institutions comply with data protection rules both when they process personal data themselves and when they develop new EU policies. In the case of the former, it means acting as a supervisory authority for all EU institutions and bodies, while the latter sees the EDPS adopt the role of an advisor to the EU legislator.

Much of our work in 2018 focused on ensuring that both the EDPS and the EU institutions and bodies we supervise were prepared for the [new data protection rules](#), which became fully applicable on 11 December 2018. In line with the action points set out in the [EDPS Strategy](#), a particular focus of our work has been on

increasing [accountability](#), ensuring that all EU institutions, including the EDPS, are capable of not only complying with data protection rules, but of demonstrating this compliance.

In addition to this, we continued to fulfil our standard obligations as a supervisory authority for the EU institutions. These include issuing recommendations to individual institutions in the form of [prior-checking Opinions](#), dealing with [complaints](#), carrying out regular audits and compliance visits and providing relevant training sessions on the new Regulation.

A second action point set out in the Strategy commits the EDPS to facilitating responsible and informed policymaking. Among the tools we have for doing this are our [Opinions](#) and [Formal Comments](#). These allow us to provide specific recommendations on EU legislative proposals. Our efforts in 2018 included 11 Opinions, 14 sets of formal comments and over 30 informal consultations on draft proposals by the Commission. These numbers clearly demonstrate the increased need for, and relevance of, independent expert advice on the data protection implications of EU initiatives, as well as growing interest from EU institutional stakeholders.

With new technologies appearing every day, we are dedicated to ensuring that the data protection field takes the necessary steps to adapt to the digital era. EDPS initiatives such as the [Internet Privacy Engineering Network](#) (IPEN) aim to reinforce the new rules set out in the [General Data Protection Regulation](#) (GDPR) and encourage the development of privacy-friendly technologies.

We recognise that data protection alone cannot solve every problem, so to ensure that data protection goes digital we have also focused on developing cross-disciplinary policy solutions. Through initiatives such as the Digital Clearinghouse, for example, we hope to encourage increased cooperation between data protection and consumer protection authorities to ensure individuals' rights are adequately protected.



#### 4.4.1 The DPO function: EU institutions leading by example

[Data Protection Officers](#) (DPOs) from the 66 EU institutions, bodies, agencies and offices meet with the EDPS twice a year, as part of their DPO network meetings. These meetings reinforce collaboration between the DPOs and ensure that the EU institutions have the tools they need to lead by example in the application of data protection law.

With new data protection rules for the EU institutions under discussion, recent meetings have focused almost exclusively on helping the DPOs to ensure that they are ready for the new rules. This year's first meeting, which took place in Brussels on 31 May 2018, was no exception.

Just a week before the 43<sup>rd</sup> DPO meeting, the GDPR became fully enforceable and the Council announced a political agreement with the European Parliament on a GDPR for the EU institutions ([see section 4.1.2](#)). Unsurprisingly then, the day's activities focused on ensuring that DPOs were equipped with all the necessary knowledge and tools not only to ensure compliance with the new rules, but to demonstrate this compliance, through applying the principle of accountability. With the aim of providing them with practical examples of how to apply the new rules, DPOs took part in several interactive exchanges, focused on specific case studies. These covered many topics, including social media and micro-targeting, data protection impact assessments (DPIAs) and IT governance.

To provide further support to the DPOs in the transition to the new rules, on 30 September 2018 we published an [updated version](#) of our 2005 position paper on the role of DPOs within the EU institutions. This paper also covers their relationship with the EDPS and provides guidelines on the profile of a DPO and the resources required for them to perform their role. The updated version brings the paper in line with the new rules set out in Regulation 2018/1725 and incorporates feedback from DPOs, gathered during a consultation period in spring 2018.

The new rules became fully applicable on 11 December 2018. On 12 December 2018, DPOs gathered once more in Brussels for the 44th EDPS-DPO meeting. The meeting was a chance to reflect on the new challenges faced by the EDPS and DPOs under the new legislation.

We planned the day's activities around a series of case studies aimed at providing the DPOs with hands-on experience of how to deal with some of these new challenges. These included the restriction of individuals'

rights under the new rules, data breach notifications and joint controllership. We wanted to encourage the DPOs to see the new rules not as a burden, but rather as a reference tool on how to ensure respect for the rights of those individuals whose personal data the EU institutions use on a daily basis to carry out their tasks and responsibilities.

Before both DPO meetings, we organised an additional training session for recently-appointed DPOs and Assistant DPOs. The new DPOs were given useful information about their role and responsibilities, ending the day with a practical case study to put their knowledge into practice.



#### 4.4.2 Reinforcing the accountability of EU institutions

Both the GDPR and the new data protection rules for the EU institutions stress the importance of accountability. This is the idea that the data controller, the person or organisation responsible for processing personal data, must not only comply with data protection rules, but be able to demonstrate this compliance. It is not a new concept, but the new rules place greater emphasis on it.

Accountability involves doing the right thing, for the right reasons, in a way that can be reproduced if required. In order to make this a reality, every organisation operating within the EU, including the EU institutions, must ensure that they adequately document all of their data processing activities.

To help the EU institutions with this, we issued an [accountability on the ground toolkit](#). A preliminary version of the toolkit was published in February 2018, to help the EU institutions in their preparations for the

new rules. An updated version, which accurately reflects the final version of the new Regulation 2018/1725, was issued in December 2018, to coincide with the day on which the new rules became fully applicable.

The toolkit provides guidance on how to document a processing operation, through what are known as records. It also sets out the criteria for determining when a DPIA, or threshold assessment, is required.

The toolkit complements the work on accountability we have been doing with DPOs ([see section 4.4.1](#)), as well as the training sessions and accountability visits we have carried out over the past two years to prepare the institutions for the new Regulation ([see section 4.1.2](#)).

#### 4.4.3 Accountability in IT

Two months before the GDPR became enforceable, we issued two new sets of Guidelines. These Guidelines provide the EU institutions with advice on how to adapt to this new era in data protection, notable for the emphasis it places on the principle of accountability.

The Guidelines address data protection requirements for the [management and governance of IT infrastructure](#) in general, and for [cloud computing services](#) specifically. Published before the new rules for the EU institutions had been finalised, the Guidelines build on the principles outlined in the GDPR and complement our other efforts to prepare the EU institutions for the new rules ([see sections 4.1.2, 4.4.1 and 4.4.2](#)).

We fully support the idea that the EU institutions should benefit from the newest technological developments. Doing so will ensure that the EU administration is both efficient and transparent. The Guidelines aim to demonstrate that this can be done while maintaining full respect for fundamental rights. They clearly identify the limits which must be respected.

In advance of the publication of these Guidelines, we were invited to a [workshop on security of personal data processing](#) to present our provisional guidance for the EU institutions on documentation and obligations relating to DPIAs and the role played by [IT security risk management](#) in this.

Organised by the EU Agency for Network and Information Security (ENISA) and Italian [data protection authority](#) (DPA) Garante, the workshop took place in Rome on 8 February 2018. A focus of the discussion was on the need for organisations to better integrate personal data protection risk management into their working methods.

Integrating new obligations relating to both DPIAs and IT security into a common risk management process which addresses both IT security and data protection risks is undoubtedly a challenge. However, it avoids duplication and allows for a more successful implementation of the obligations outlined in the GDPR, making it much more efficient than implementing separate processes.



#### 4.4.4 Data breach notifications: a how-to guide for EU institutions

To help the EU institutions with their preparations for the new rules (see sections 4.1.2, 4.4.1 and 4.4.2) we issued [Guidelines on Personal Data Breach Notification](#).

Under the new Regulation, all EU institutions and bodies have a duty to report certain types of personal data breaches to the EDPS. They must do this within 72 hours of becoming aware of the breach. If there is a high risk that the breach will adversely affect individuals' rights and freedoms, the EU institution must also inform the individuals concerned without unnecessary delay.

The costs and risks related to a data breach can be significant. Since the first mandatory data breach notification law was passed in California in 2002, the obligation to notify different types of breaches has spread across the world, in response to an increasing number of incidents. This obligation should not only act as a deterrent but also encourage organisations to do everything in their power to prevent breaches from occurring in the first place. The GDPR's strict requirements on data breach notifications have already demonstrated the positive effects of this approach.

With the new data protection Regulation for EU institutions now in force, the institutions must ensure they have prevention and detection mechanisms in

place for personal data breaches, as well as investigation and internal reporting procedures. The new Guidelines provide the necessary practical advice and background information for assessing and notifying the EDPS through a [new online form](#), which can be found on [our website](#).

#### 4.4.5 Protecting privacy in the EU institutions

One of the main duties of the EDPS is to hear and investigate complaints and conduct inquiries.

In 2018, the EDPS received 298 complaints, an increase of 111% compared to 2017. Of these, 240 complaints were inadmissible, the majority relating to data processing at national level as opposed to processing by an EU institution or body.

The remaining 58 complaints required in-depth inquiry, an increase of 132% compared to 2017.

In addition, 38 cases submitted in previous years were still in the inquiry, review or follow-up phase on 31 December 2018 (one in 2012, seven in 2014, three in 2015, twelve in 2016 and fifteen in 2017). In 2018 we issued 23 complaint decisions.

#### Data protection for conference organisation

On 10 April 2018, we responded to a complaint regarding the registration process for an international conference organised by one of the EU institutions. This process required individuals to submit a scanned copy of their passport or identity card, in order to verify their identity.

Our investigation found that the EU institution could have used a less intrusive means of verifying the identity of participants, such as checking passports or ID cards at the entrance to the conference and comparing them with the information submitted online. We also noted that in certain Member States it is illegal to photocopy passports unless justified by the law.

Furthermore, the EU institution failed to formally notify their DPO of the collection of scanned copies of individuals' ID, as was required under [Regulation](#)

[45/2001](#), the data protection rules applicable to the EU institutions at the time of the complaint.

We also responded to concerns about the transfer to the authorities of the host Member State of the personal data collected by the conference organisers. The EU institution claimed that this transfer was carried out on the premise that participants had consented to it. However, to qualify as a valid legal basis for the transfer of data, consent must be freely given. As participants were not able to register for this conference unless they gave their consent to share personal information with the host Member State authorities, their consent was not freely given. As a result, consent, in this case, cannot be considered a valid legal basis for the transfer of data.



#### Data processing for social media monitoring

On 21 March 2018, we adopted an [Opinion](#) on the processing of personal data for social media monitoring at the European Central Bank (ECB). The ECB intended to use an external contractor to monitor and track discussions about ECB related topics on different social media channels. Their aim was to gain a better understanding of how internet users perceive the ECB and to improve the ECB's communication and reputation.

Specifically, the ECB wanted to collect information on what was being said about them, topics related to their activities, the tone used and how far the information

was spread. The monitoring and analysis of the aggregated data on different groups of users was to be carried out by the external contractor, while the ECB would analyse this information and draft reports.

As some internet users, who are not public figures, may be indirectly identifiable by their quotes, their likes or their native language, we provided the ECB with some specific recommendations aimed at ensuring that the rights of individuals would be respected. In particular, we focused on the need to ensure the quality of the data collected and processed, provided recommendations on the content of the contract with the external contractor and advised the ECB on an individuals' right of access to their own data. We also provided them with advice on the information they must provide to internet users and the security measures the contractor must adopt.

On 13 November 2018, we carried out an in-situ inspection at the ECB and were very happy to note that the ECB had put our recommendations into practice. In addition, almost all data used by the ECB communication team is now aggregated.

Under Regulation 45/2001, all processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes were to subject to prior checking by the EDPS.

In 2018, we received ten notifications for prior checking, a 92% reduction on 2017. We issued 90 prior check Opinions, an increase of 55% from 2017. Of these, seven were Non-Prior Check opinions and three were updated Opinions following updated notifications. 90% of the risky processing operations that we were notified about in 2018 related to administrative procedures, such as recruitment of staff, staff annual appraisals or the conduct of administrative inquiries and disciplinary procedures, as has been the trend in past years.

## Number of complaints received

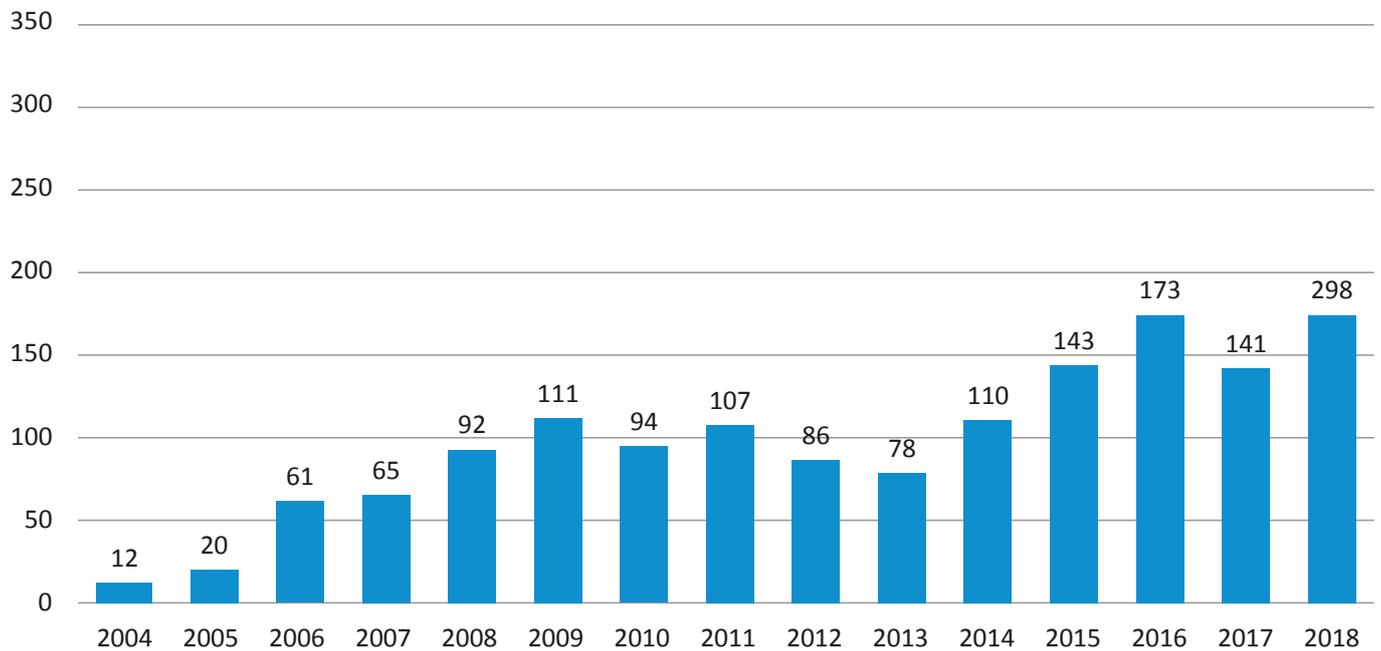


Figure 3. Evolution of the number of complaints, including inadmissible complaints, received by EDPS

## EU institutions and bodies concerned

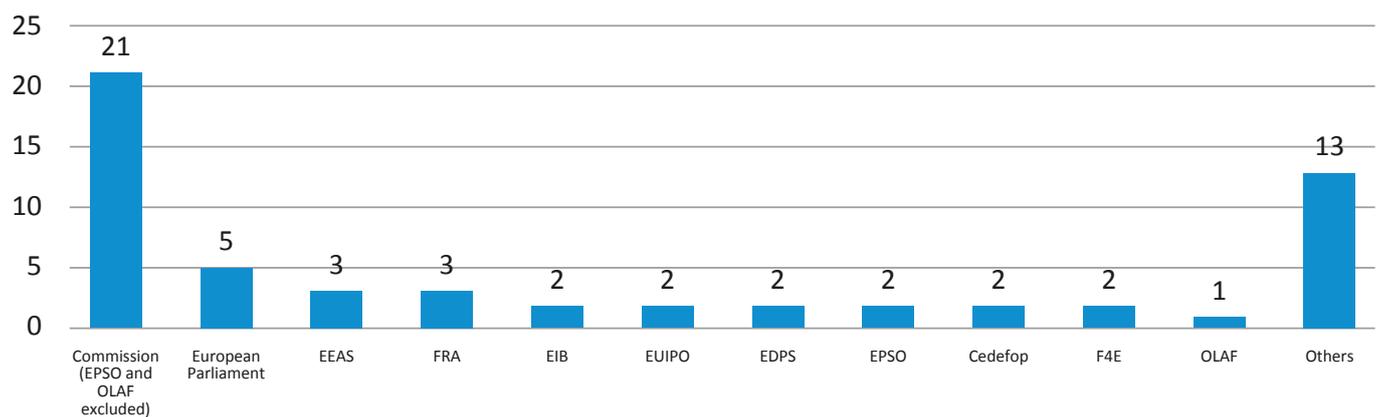


Figure 4. EU institutions and bodies concerned by complaints received by EDPS

## Topics of complaints 2017

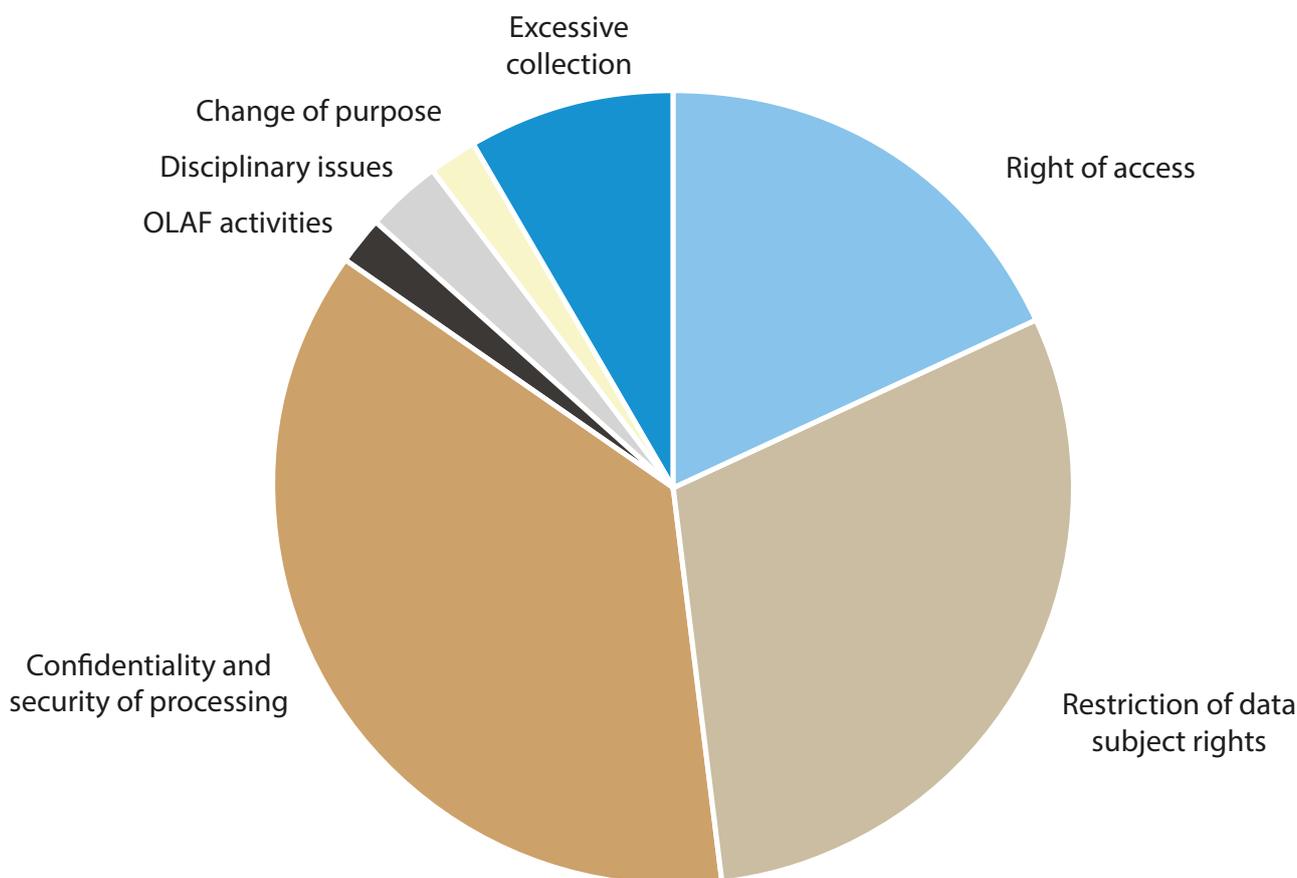


Figure 5. Type of violation alleged in complaints received by EDPS

In 2018 we received ten consultations on administrative measures (eight under Articles 28.1 of Regulation 45/2001 and two under Article 41 of Regulation 2018/1725).

We received 30 consultations, (29 under Article 46(d) of Regulation 45/2001 and one under Article 57(1)g of Regulation 2018/1725), eight of which were informal consultations.

### Joint controllership: the case of the Online Linguistic Support tool

Erasmus+ is the European Commission's programme for education, training, youth and sport. The Education, Audiovisual and Culture Executive Agency (EACEA) runs the programme for the European Commission's Directorate General for Education and Culture (DG EAC), alongside national agencies in the Member States.

As part of the Erasmus+ programme, EACEA runs an online tool known as Online Linguistic Support (OLS). It is used to check if an individual's language skills have improved during their stay abroad. Language skills are tested both before an individual leaves their home country and upon their return home. OLS also provides online language classes. The tests are mandatory for any individual receiving funding through Erasmus+, but any consequences relating to failing to take the test, such as a reduction in an individual's mobility grant, are decided at national level.

Any processing of personal data proposed by an EU institution or body and considered to pose a specific risk to the rights and freedoms of the individuals concerned is subject to prior checking by the EDPS. However, while EACEA provides the online tool, it does not carry out an evaluation of the data collected by the tool. This is done at national level. We therefore informed EACEA that no prior check was necessary in this case.

## Notifications to the EDPS

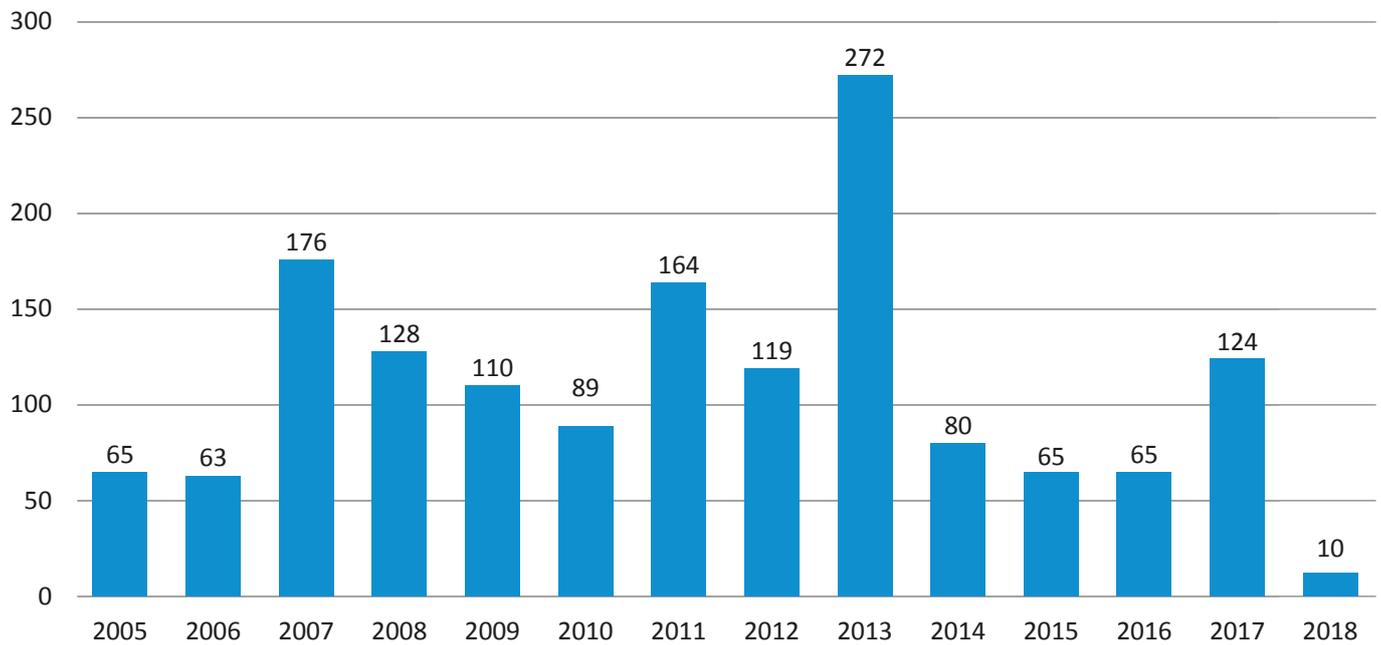


Figure 6. Evolution of Notifications received by EDPS

## EDPS prior check Opinions per year

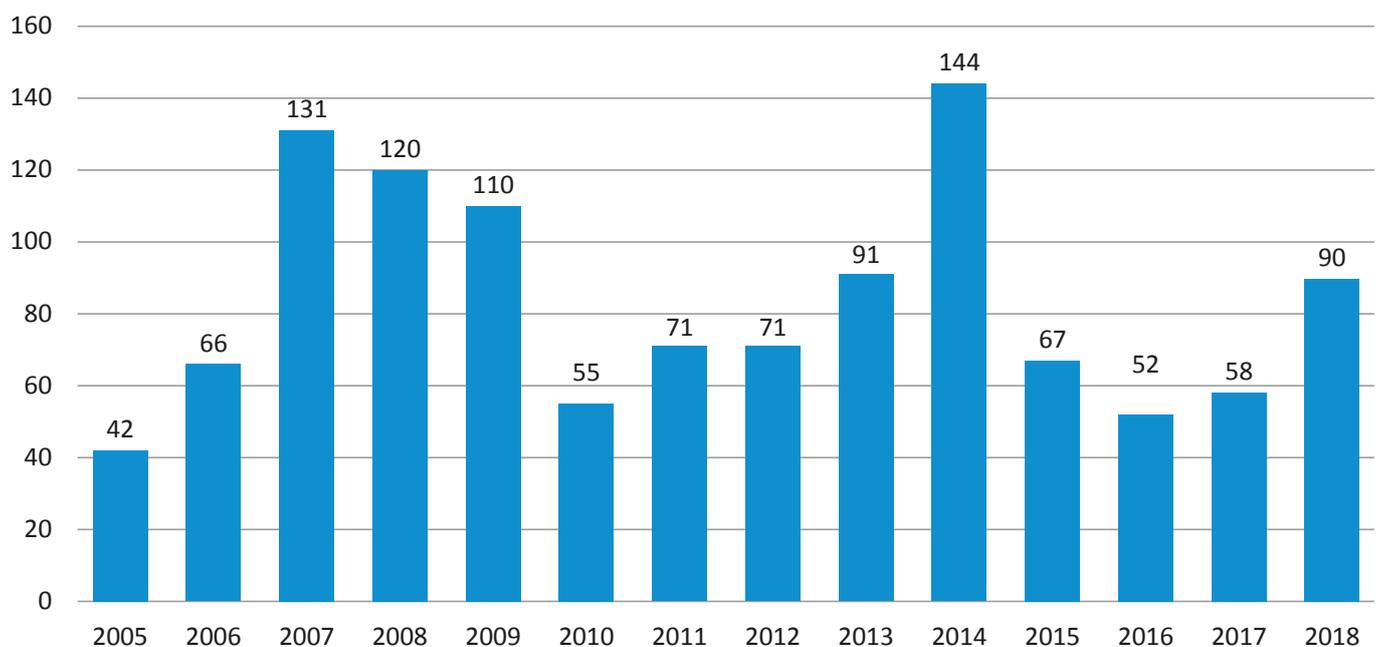


Figure 7. Evolution of prior check Opinions issued by EDPS

## Notifications to the EDPS 2018 Core Business vs Administration

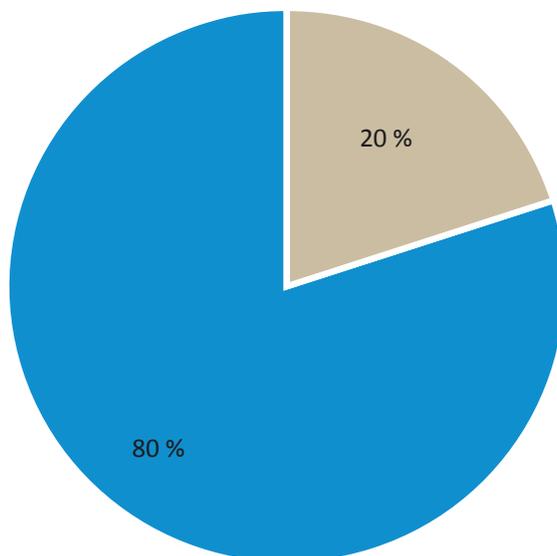


Figure 8. Percentage split between Core Business and Administration activities in the Notifications received by EDPS

The case raised an interesting question, however, which is relevant to many European systems, platforms and tools.

The EDPS sees the distribution of tasks between EACEA and DG EAC on the one hand, and national agencies on the other, as a case of joint controllership. This means that both EU and national authorities are responsible for determining the means and purposes of the processing of personal data. We therefore recommended that these joint controllers clarify their respective responsibilities, so that it is possible for individuals to address the right organisation immediately, depending on their needs. For example, in the case of the OLS, requests for access to personal data relating to test results should be addressed to the national agency of an individual's home country, while the security of the OLS central system remains the responsibility of EACEA.

### EU trade unions and the EDPS

On 29 January 2018, we responded to a consultation from a trade union for EU staff, relating to the conditions for sharing data within the same trade union.

Our Opinion found that these trade unions are not classified as EU institutions or bodies under the relevant provision of the rules for the EU institutions and bodies, set out at the time under Regulation 45/2001.

Nevertheless, as a general rule, any internal transfer of data should be governed by the need-to-know principle. We therefore advised the trade union to carry out an analysis to determine whether or not internal data transfers were necessary in this case.

### EU institution websites must lead by example

The EDPS has received a number of complaints relating to the protection of privacy and personal data on the websites of certain EU institutions and bodies. These complaints related to:

- the use of third-party services;
- user consent relating to cookies;
- the information provided to website users in the website's cookie policy;
- the information provided to users in the website's privacy policy.

We have been working closely with the institutions concerned to resolve any possible issues raised in the complaints. This fits with our broader efforts to help all EU institutions and bodies ensure compliance with the applicable data protection laws, including our attempts to help them better protect the users of

their websites. Included in this is our programme of remote inspections (see section 4.4.7) and the organisation of specific training sessions (see figure 2), among other activities. These efforts will continue into 2019 as we aim to ensure that every EU institution website complies with the relevant data protection requirements.

#### 4.4.6 Catching up with the institutions: audits and visits

Audits and visits are two of several tools we use to monitor the EU institutions and ensure that they abide by the relevant data protection rules. Visits are also a useful tool in helping to raise awareness about data protection in the EU institutions and have proved particularly useful as part of our campaign to raise awareness and help prepare the EU institutions for the new data protection rules (see section 4.1.2).

We carried out seven audits and three compliance visits in 2018. With the new rules in mind, these were aimed at ensuring that the EU institutions have the right tools and knowledge to move beyond mere compliance,

towards the approach based on accountability outlined in the new Regulation. It is vital that the EU institutions are able to lead by example in their application of data protection rules in order to help ensure the success of the GDPR EU-wide.

The results of audits are always shared directly with the institutions concerned. We then follow up in due course to ensure that our recommendations have been put into practice. Compliance visits, on the other hand, involve working with the respective EU institution to draw up a roadmap for compliance. We then follow up with the institution to ensure that the roadmap has been effectively implemented.

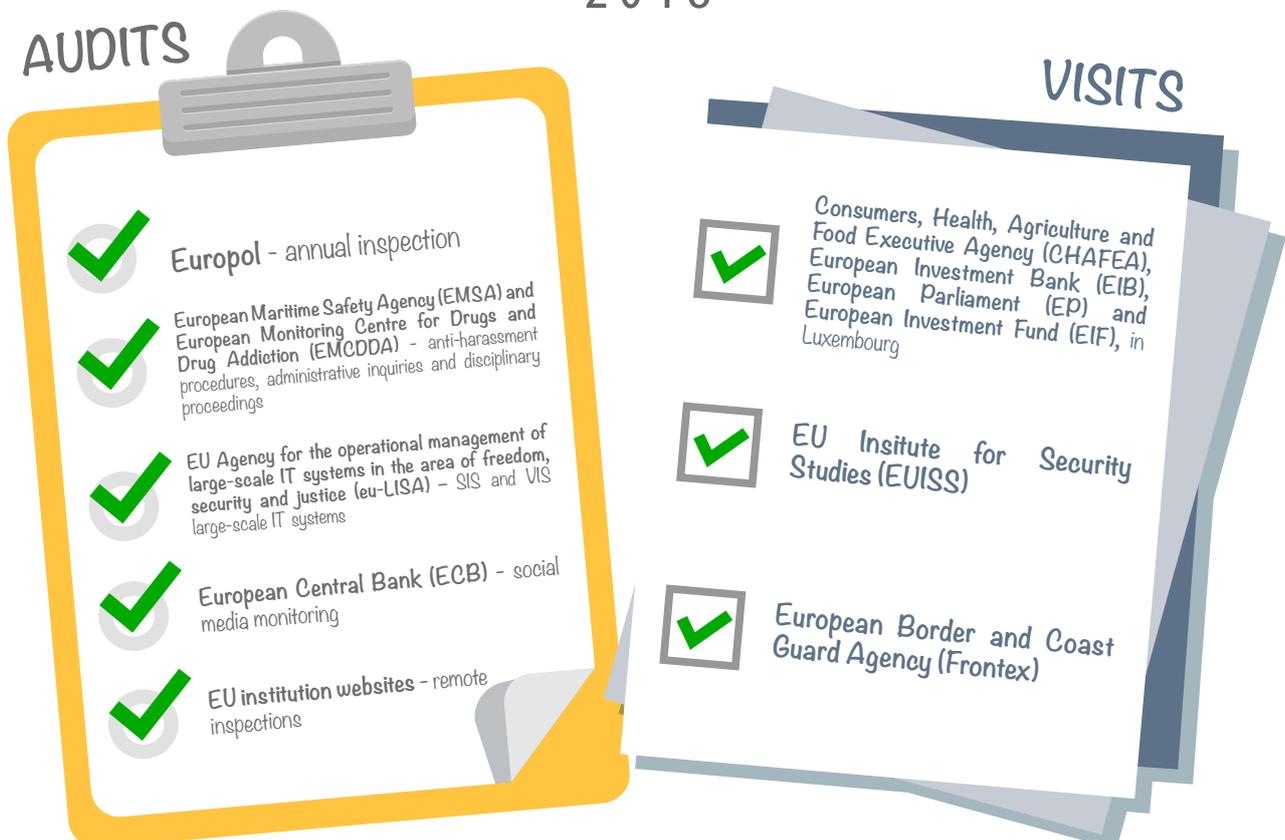
Under the new Regulation 2018/1725, we will continue to carry out audits and visits. The emphasis will remain on encouraging and ensuring an approach to data protection based on accountability, in line with the new rules.

#### 4.4.7 Remote inspections of webservicees

In November 2016, we published [Guidelines](#) on the protection of personal data processed through web services provided by EU institutions. In July 2018, we

## EDPS audits and visits

### 2018



began a follow-up exercise, consisting of remote inspections of the web services offered by the EU institutions.

Remote inspections involve the remote scanning of web services, and can therefore be carried out on EDPS premises. Our approach is comprehensive, taking into account all of the web services offered by the EU institutions. For the first time in the history of the EDPS, we also automated part of the evidence collection and documentation.

As the number of web services reported by the institutions totals more than 700, we have organised the inspections in waves. Each wave is composed of a set of web services, with the first wave including those services likely to have the highest impact on the individuals using them.

The first inspection wave, which included the web services of the largest EU institutions as well as two Europol websites (see section 4.2.3), is now complete, while the second wave is due to finish in early 2019. Further inspection waves will take place throughout the coming year.

The results of the first inspection wave were welcomed by the EU institutions, triggering actions that have greatly improved their web service compliance. We hope to see a similar response to the results of future waves.

#### 4.4.8 Transparency, re-use and data protection

This year's annual Forum of Official Publishers took place on 8 June 2018, in Oslo, Norway. Our participation in this event is a good opportunity for us to demonstrate how data protection works in practice, when applied to official publications.

In our contribution, we reported on our experience and expertise as an advisor to the EU legislator, as the supervisor of the EU institutions and as the supervisor of the Publications Office of the European Union in particular. Our aim was to provide practical guidance on how to ensure compliance with data protection principles and rules when dealing with official publications.

We focused on three key topics aimed at helping publishers to navigate the GDPR:

- The role of publishers in relation to personal data when they publish on behalf of national Courts, Justice Ministries or Parliaments. Specifically, we focused on clarifying the situations in which the

publisher acts as a controller of personal data and when they act as a processor.

- The right to erasure, also known as the right to be forgotten, including the conditions under which it applies and the limits to this right.
- The data protection safeguards in place in case of the re-use of public sector information, allowed for under Directive 2003/98.

The event was also an opportunity to improve our engagement with Norway, a European Economic Area (EEA) country to which the GDPR applies, and with Japan, who attended the conference to give a presentation as an official publisher. The group expressed an interest in hearing updates on data protection matters as part of its future annual meetings.

#### 4.4.9 Cross-border investigations of a different kind

Ever since the GDPR became enforceable on 25 May 2018, some EU institutions have experienced problems collecting required information from certain companies. These companies claim that the GDPR prevents them from providing the EU institutions with this data. Some of the institutions and bodies affected by this problem include:

- the European Commission's Directorate General for Competition (DG COMP), which works, among other things, on anti-trust matters;
- the European Anti-Fraud Office (OLAF), which carries out external investigations on suspected fraud;
- the European Investment Bank (EIB) and European Investment Fund (EIF), which need to audit funded projects.

In response to this problem, we made sure that the EU institutions concerned were fully informed about the law and how it is relevant to their work.

The collection of data necessary for fulfilling the task assigned to them by law is legal, and not restricted by the GDPR. The relevant EU institution or body is obliged to inform the individual concerned that they plan to process their personal data, but there are also exceptions to this rule, principally where informing the individual involved would jeopardise the investigation, particularly in its early stages.

However, the EDPS is unable to resolve this problem alone. This is because the main issue here concerns the obligations of the companies, who are controllers

under the GDPR. As it is the job of national DPAs to supervise adherence with the GDPR within their respective countries, we turned to the European Data Protection Board (EDPB) (see section 4.1.1) to follow up on this matter. We hope to have a resolution to the problem as soon as possible.

#### 4.4.10 Application for Return

Frontex Application for Return (FAR) is a platform which enables the exchange of information on returnees between the European Border and Coast Guard Agency (Frontex) and the Member States. Returnees are individuals from a non-EU country considered to be staying illegally in the EU and subject to a return decision issued by a Member State, through either an administrative or judicial procedure. The platform would allow Member States to inform Frontex about their return operations, including the number of returnees and where they will be returned to, as well as any type of material assistance they might require from Frontex.

On 26 September 2018 we issued a prior-checking Opinion on the FAR platform. We made a number of recommendations with specific reference to the data protection notice associated with this processing operation and to the need to ensure that all returnees are guaranteed the rights of access to and rectification of their personal data. We also stressed the need to carry out risk assessments in relation to the restriction of rights and in the field of IT security and anonymisation.

Return operations involve data processing operations where the individual concerned is particularly vulnerable. It is therefore vital to ensure that data protection principles are respected in order to preserve the dignity of these individuals.

#### 4.4.11 Security verifications of external contractors

EU institutions often use external contractors to provide certain services, such as cleaning, security or IT. However, it is essential to ensure that these external contractors do not introduce security risks. In Belgium, some EU institutions do this by carrying out a security screening process in cooperation with the Belgian authorities.

Though a number of EU institutions had developed procedures relating to this screening process, others were less well-informed. On 30 October 2018, in response to a request from the European External Action Service (EEAS), we issued an Opinion on the topic in which we outlined several recommendations aimed at helping the EU institutions.

The Opinion stressed the importance of establishing a proper legal basis for carrying out the screening process, such as that put in place by the European Commission. EU institutions must also ensure that the individuals concerned are adequately informed about how both the relevant EU institution and the Belgian authorities will process their personal data and that they are made aware of their right to challenge any decisions made against them.

#### 4.4.12 Supervising the EFTA Surveillance Authority

In October 2017, we took on the role of data protection supervisor for the EFTA Surveillance Authority (ESA). ESA's main task is to ensure that the European Free Trade Association (EFTA) countries of Iceland, Norway and Lichtenstein respect their obligations under the European Economic Area Agreement.

EU data protection legislation also applies to the EEA. The EFTA countries are therefore required to establish independent national supervisory authorities to enforce the GDPR. However, the GDPR does not apply to EFTA institutions. As a result, even though EFTA institutions were exchanging personal data with the European Commission and other EU bodies on a regular basis, they were not subject to any data protection rules or supervision.

The special supervisory regime agreed upon in late 2017 closed this legal vacuum. It consists of:

- ESA Decision 235/16/COL, based on the data protection rules for EU institutions set out in Regulation 45/2001, with minor changes to reflect the specific legal and operational environment in which ESA operates. This Decision provides for the supervisory role of the EDPS.
- A Memorandum of Understanding (MoU) between ESA and the EDPS, establishing our powers and tasks as ESA's data protection supervisor.

However, with the introduction of new rules for the EU institutions, this special supervisory regime is now out of date. In spite of [our recommendations](#) to the contrary, Regulation 2018/1725 does not cover data protection rules or supervision for the EFTA institutions.

With the EU institutions and bodies now bound by the new rules, it follows that ESA's data protection regime must be updated, to bring it in line with these rules. Only through doing so will we be able to ensure the adequate protection of personal data in exchanges with the EFTA institutions.

#### 4.4.13 Eurojust: a new supervisory role for the EDPS

The European Union Agency for Criminal Justice Cooperation (Eurojust) was set up to reinforce the fight against serious organised crime within the EU and to promote coordination and cooperation between national investigating and prosecuting authorities dealing with these crimes.

On 6 November 2018, the European Parliament and the Council adopted a new legal framework for Eurojust. It includes new rules on data protection, which task the EDPS with supervising the processing of personal data at Eurojust. It also provides for cooperation between the EDPS and the national DPAs within the framework of the EDPB on any issue requiring national involvement, in order to ensure coordinated supervision. Our new supervisory responsibilities will begin on 12 December 2019.

To prepare for this new supervisory role, we will coordinate internally and organise regular meetings with the DPO of Eurojust. The relevant EDPS staff members will also follow internal and external training sessions related to Eurojust supervision.

A first visit to the headquarters of Eurojust in The Hague took place on 29 November 2018 and more visits are planned in 2019, in order to ensure a smooth transition to EDPS supervision of Eurojust's data processing activities.

#### 4.4.14 Advising the EU institutions



##### Free and fair European elections

On 17 December 2018, we published an [Opinion](#) on the European Commission's legislative package on free and fair European elections. The package consisted of four parts:

- a Proposal for a Regulation concerning a verification procedure for infringements of rules on the protection of personal data in the context of the European Parliament elections;
- a European Commission Communication on securing free and fair European elections;
- a European Commission Recommendation on election cooperation networks, online transparency and protection against cybersecurity incidents and fighting disinformation campaigns relating to the European Parliament elections;
- a European Commission Guidance document on the application of Union data protection law in the electoral context.

In our Opinion, we recognised the fact that the package underlined the role of social media platforms in the election process, as well as the consistency of the package with the Commission's [Code of Practice on online disinformation](#).

With European Parliament elections set for May 2019 and numerous other national elections scheduled throughout the year, we acknowledged the need to set up national election networks and a European coordination network, as outlined in the Commission's Recommendation. Given our work in this area, we also expressed our interest in participating in the European network.

Our Opinion reinforced the urgency of the Commission's call for Member States to assess the risks associated with the European Parliament elections, particularly potential cyber incidents that could affect the integrity of the electoral process.

Moreover, we felt that, for further clarity, a reference could have been included to the fact that personal data processed by the European Parliament, the Authority for European political parties and European political foundations and the Committee of independent persons will be done within the scope of the new Regulation for the EU institutions and bodies ([see section 4.1.2](#)).

We also provided several specific recommendations on the proposed Regulation, including the need to clarify the scope of the new measures and their aims and the need to ensure confidentiality in the exchange of information between DPAs and the Committee of independent persons. In addition, we advised including references to EDPS decisions and the current data protection legal framework.



@EU\_EDPS

Personal [#data](#) is an aspect of human [#freedom](#) and [#dignity](#), its protection is a [#FundamentalRight](#). Extending consumers protection should be pursued with this in mind. Time for a closer and systematic cooperation between the [#consumer](#) and [#dataprotection](#) authorities

### A new deal for consumers

On 5 October 2018, we published an [Opinion](#) on the legislative package *A New Deal for Consumers*. The package consisted of the Proposal for a Directive as regards better enforcement and modernisation of EU consumer protection rules and the Proposal for a Directive on representative actions for the protection of the collective interests of consumers.

The EDPS has [consistently called](#) for a coherent approach to enforcement from authorities responsible for the digital economy and society. These include consumer, data protection and competition authorities. We reiterated this in our Opinion, stressing that consumer law and data protection can no longer afford to work in insolation. A big-picture approach to addressing systemic harms to individuals in digital markets is required, involving closer cooperation between enforcers in order to avoid legal uncertainty.

We welcomed the initiative to update the enforcement of consumer rules and supported the package's aim to extend benefits to consumers who receive services without paying a monetary price. However, with *free* the preferred price for many digital markets, the consumer should be protected regardless of whether a contract to provide digital content or services requires payment or not.

Both consumer and data protection law must be effective in tackling any harm arising from the digitisation of people's lives. Personal data cannot be treated as an economic asset. It is therefore vital to ensure that personal data is not mentioned in contract definitions for the supply of digital content or a digital service, in line with the safeguards provided

for by the [Charter of Fundamental Rights](#) and the GDPR.

Closer alignment between consumer and data protection requires policymakers, as well as regulators, to deepen their dialogue and understanding. Initiatives such as the Digital Clearinghouse ([see section 4.4.18](#)) and the joint meetings of the EDPB and the Consumer Protection Cooperation Network are vital steps towards achieving this.



### Rules on re-using Public Sector Information

On 10 July 2018 we issued an [Opinion](#) on the European Commission's Proposal for a new Directive on the re-use of Public Sector Information (PSI). In proposing to amend the [current Directive](#), the Commission was looking to facilitate the re-use of PSI throughout the EU by harmonising the basic conditions for re-use.

PSI data includes legal, traffic, meteorological, economic and financial data. Our Opinion provided specific recommendations on how to clarify the relationship between the proposed PSI Directive and the exceptions outlined in the GDPR. We also addressed how to deal with the cost of data anonymisation and the use of DPIAs for *sensitive sectors*, such as healthcare.

In particular, we specified that precise wording be used to better clarify the coherence between the PSI Directive and the GDPR. Furthermore, due to the high costs associated with anonymising personal data, we suggested that every organisation falling within the scope of the PSI Directive should be able to charge for anonymisation expenses.

We also stressed the importance of protecting the rights of individuals. While it may be true that more data than ever is now generated and processed by machines, much of it still falls within the definition of personal data. For this reason, we specifically highlighted the various

challenges arising from trying to differentiate between personal and non-personal data.

### Digital tools and processes in company law

On 25 April 2018, the European Commission adopted a proposal amending EU Directive 2017/1132 on the use of digital tools and processes in company law. In response to separate requests from both the Commission and the Parliament, we published an [Opinion](#) on the proposal on 26 July 2018.

The proposal sets out rules for online company registration and the electronic filing and publication of registered information on companies and branches and therefore entails the exchange of personal data. For example, information about the founder of a company or its director might be submitted in an online registration and electronically filed.

The proposal also provides for free of charge access in all Member States to a list of documents and information, the establishment of an optional access point to the platform for the EU institutions, and would introduce the *once-only principle* in the area of company law. The once-only principle would mean that companies would only have to submit relevant information once, to be shared with different authorities if required. Personal data would therefore also be accessible to various national authorities in business registers, as well as in documents required for cross-border operations such as mergers, divisions and conversions.

Additionally, the proposal would allow for the exchange of data on the disqualification of directors between national business registers. Such an exchange is likely to involve data relating to criminal convictions and offences. As this is considered as sensitive data, it requires appropriate safeguards.

We outlined several recommendations aimed at ensuring the highest level of protection for all personal data concerned. The proposal is now under negotiation in the Council and the European Parliament.

#### 4.4.15 New technologies

##### Blockchain: assessing the implications for data protection

*Blockchain* has become a powerful buzzword in the world of technology and financial innovation. The technology is currently used as an enabler for Bitcoin and other so-called *crypto-currencies*, and sparked the development of [Distributed Ledger Technology \(DLT\)](#).

Distributed ledgers such as blockchains are databases with many replicas under the shared control of distinct, often autonomous, participants.

Originally developed to secure online transactions through the use of sophisticated cryptography, EU industries and legislators are now assessing the viability of using blockchain in a variety of areas, from finance to e-government and even in personal healthcare. However, it is vital to ensure that these assessments consider the data protection implications of using distributed databases.

Whenever blockchain technology is used to process personal data the relevant data protection law applies. In the EU, this law is the GDPR. We have been following the evolution of blockchain since 2016 and have so far identified a number of data protection challenges, relating to areas such as storage limitation, controllership and individual's rights, which we will look to investigate further in 2019.



#### 4.4.16 Privacy engineering gaining ground

In February 2018, Assistant Supervisor Wojciech Wiewiórowski attended the Mobile World Congress in Barcelona, one of the world's most important technology events. He participated in panels and roundtables alongside other data protection commissioners from around the world.

The event was a chance for privacy regulators to explain how data protection principles can be applied to new technology and how these principles protect the fundamental rights of citizens, while also outlining their expectations in relation to the measures taken by the industry to incorporate these principles into their products. Industry representatives, however, expressed their concerns that some legislative initiatives could lead to the unnecessary restriction of the cross-border data flows considered necessary for some business activities.

The EDPS participated in a debate with industry and consumer representatives on transparency and control for individuals in the collection and processing of their data in Internet of Things (IoT) environments. We highlighted the clear rules on this topic, outlined in the GDPR, and stressed the need for manufacturers and IoT device and service providers to adopt the principles of data protection by design and by default. To help them with this, we invited them to attend the [IPEN workshop](#), which took place in Barcelona on 15 June 2018, organised with the support of the Polytechnic University of Catalonia (UPC).

IPEN was set up by the EDPS in 2014 to promote privacy engineering and bridge the gap between legal and IT engineering approaches to data protection. As in 2017, the 2018 workshop took place immediately after the ENISA Annual Privacy Forum. The main aim of the workshop was to assess the state of play of privacy engineering and privacy-enhancing technologies (PETs) in the wake of the GDPR, and to follow up on the outcome of last year's trans-Atlantic workshop, which focused on research and development needs in privacy engineering.

IPEN participants provided updates on ongoing initiatives such as the [IPEN wiki](#) on privacy-related standardisation initiatives and the PETs maturity deposit. The relationship between ethics and technological developments was also a topic for discussion. We challenged those present to think about moving from privacy by design to the concept of human rights by design.

The Workshop provided an opportunity for businesses to present and demonstrate solutions combining innovation and data protection. Companies such as SAP, Qwant and Brave shared best practice on how to give users more control over their data. Academics reported on recent research results and presented practical tools to help detect privacy compliance issues and support regulators and controllers in implementing accountability.

The workshop marked an encouraging start to the GDPR era. We look forward to continuing this valuable interdisciplinary dialogue over the months and years to come.

#### 4.4.17 Online manipulation and personal data

On 20 March 2018, we published an [Opinion](#) on online manipulation and personal data. The Opinion responded to fevered public debate on *misinformation*,

responsible for distorting trust in the democratic process. It argued that the fundamental problem was not so-called *fake news*, but rather the abuse, on a massive scale, of personal information and the right to freedom of expression. This abuse is endemic to the *digital information ecosystem* which has evolved over the past two decades, which is dangerously complex, concentrated and lacking in explainability and accountability.

This ecosystem, often referred to as the AdTech ecosystem, depends on a cycle of constant tracking, profiling and targeting of individuals. It revolves around a handful of extraordinarily powerful platform intermediaries who, by determining what information is collected about people and presented back to them, act as effective gatekeepers for the online experience of most people today.

Restricted to commercial activities, the impact of this phenomenon on fundamental rights was already significant. Yet, as revelations from the last 12-18 months show, this volatile ecosystem has now been weaponised by actors with political motivations, including those wishing to disrupt the democratic process and undermine social cohesion. Opaque algorithmic decision-making rewards content which provokes outrage, on the basis that greater *engagement* generates revenue for the platforms in question. This poses obvious risks to fundamental values and democracy.

In our Opinion, we argued that much greater focus is needed on the role of regulators in working together to hold commercial and political players to account for how they process personal information. We identified a role here not only for DPAs, but also for competition authorities and audio visual service regulators and election monitors. New ePrivacy rules are also essential, to address market incentives and open up space for alternative business models which do not depend on constant surveillance and intrusive targeting ([see section 4.1.3](#)).

Above all, there is a need for DPAs to better collaborate with other regulators, particularly electoral and audio-visual regulators. With fears that political campaigns may be capitalising on centralised digital spaces and widely available data to circumvent existing laws, it is vital that we take action to protect the rights and interests of individuals in our digital society. We therefore proposed to hold a workshop in early 2019 and to invite electoral and audio visual regulators to participate in Digital Clearinghouse deliberations ([see section 4.4.18](#)).



#### 4.4.18 A more coherent approach to challenges in the digital ecosystem: The Digital Clearinghouse

There are natural synergies between data protection, consumer protection and competition policy. However, the authorities responsible for enforcing laws in these fields have long acted in isolation, as if these synergies did not exist. Increased cooperation between these authorities would help to improve understanding of market dynamics and to develop more coherent and consistent responses to the challenges posed by the digital economy.

The EDPS Strategy refers to the need to work across disciplinary boundaries to address policy issues with a privacy and data protection dimension. In response to our own analysis and calls from regulators to establish a space for dialogue, we launched the Digital Clearinghouse. The first two meetings of the Clearinghouse took place in 2017.

Our third meeting, which took place on 21 June 2018, was the first to welcome the participation of authorities from outside the EU. Regulators and enforcement agencies discussed topics of concern to all authorities present, including:

- the relevance of personal data in competition and consumer enforcement;
- the fairness of privacy policies and terms and conditions in free online services;
- collusive and personalised pricing and related theories of harm in digital markets;
- unethical data collection and analysis for the purpose of targeted marketing.

On 10 December 2018, 31 authorities from the EU and other countries met for the fourth time. We expanded the

scope of the meeting to include electoral regulators and discussed the impact of online manipulation on free and fair political activities, as part of the democratic process. With an emphasis on more practical cooperation, our discussions also focused on topics such as:

- the deceptive framing of a free offer as unfair practice;
- the opportunity to adopt structural remedies capable of provoking a change in current business models;
- asymmetric regulation of access data;
- the misuse of data protection by national authorities, including competition agencies, to frustrate investigations.

Authorities also debated non-price factors in competition and consumer enforcement analysis and agreed to continue parallel discussions on this, to develop a methodology to assess the real costs to individuals when the monetary cost of a service is zero or below marginal cost.

Moving forward, we aim to continue our efforts within the Digital Clearinghouse to ensure coherence in the areas of enquiry already under discussion, while also looking to contribute to and build on the work of existing networks.



@EU\_EDPS

The [#DigitalClearinghouse](#) met for the fourth time yesterday. 31 authorities from [#EU](#) and across the globe discussed common challenges in the [#digital](#) ecosystem. Read the statement adopted by the network <https://europa.eu/!NY93Mq>

#### 4.5. INTERNATIONAL AFFAIRS

In the digital era in which we are now living, everyone and everything is connected, regardless of where we are in the world. However, while personal data now flows freely across borders, data protection laws remain national or, at best, regional.

Better engagement and convergence on data protection at international level has been a subject of intense discussion for many years and Europe has assumed a leading position in shaping a global, digital standard for privacy and data protection. However, until more recently, little practical progress had been made.

Our [Strategy 2015-2019](#) positions the EDPS at the forefront of this discussion. At the beginning of the present mandate we committed to forging global partnerships with the aim of building a global social consensus on the principles relating to data protection.

One way in which we have sought to achieve this objective is through working with our international and regional partners to mainstream data protection into international agreements. Our work with the Council of Europe and international organisations is a good example of this, as are our efforts to ensure that EU agreements on international data transfers, such as the Privacy Shield, fully respect the fundamental rights of the EU.

#### 4.5.1 International data transfers

##### The EU-US Privacy Shield

The EU-US Privacy Shield has been in place since 1 August 2016. It is what is known as an *adequacy decision*, providing for a legal basis for the transfer of personal data from the EU to the US. The Privacy Shield is reviewed on a yearly basis, to ensure that it is implemented effectively, in a way that provides for adequate protection of personal data, in line with EU rules.

The second yearly review of the EU-US Privacy Shield took place on 18 and 19 October 2018. A team of representatives from the EU's [data protection authorities](#) (DPAs), including a representative from the EDPS, took part in the review. A report on the results of this joint review is to be adopted at the January 2019 Plenary meeting of the European Data Protection Board (EDPB).



##### An adequacy decision for Japan

In September 2018, the European Commission published a draft adequacy decision for the transfer of personal data from the EU to Japan. Before adopting the decision, the Commission was required to consult the EDPB for an Opinion.

The EDPB adopted this Opinion on 5 December 2018, using its updated guidance document on adequacy decisions as a benchmark. As the first adequacy decision of the GDPR era, the EU-Japan adequacy decision will not only set the tone for any future adequacy decisions, but may also have an impact on the upcoming review of all adequacy decisions currently in place.

The Commission also consulted the EDPS and, on 4 September 2018, we provided preliminary informal comments on the draft decision. However, in contrast to our approach to the draft EU-US Privacy Shield in 2016, we did not issue an Opinion. This is because, as a member of the EDPB, we actively contributed to discussions on the EDPB Opinion, drawing particular attention to the role of the Board and the Commission's accountability for adequacy decisions. Convinced that the EDPB Opinion represented a reasonable reflection of the Board's discussions, we encouraged the Commission to take its observations and recommendations into account.



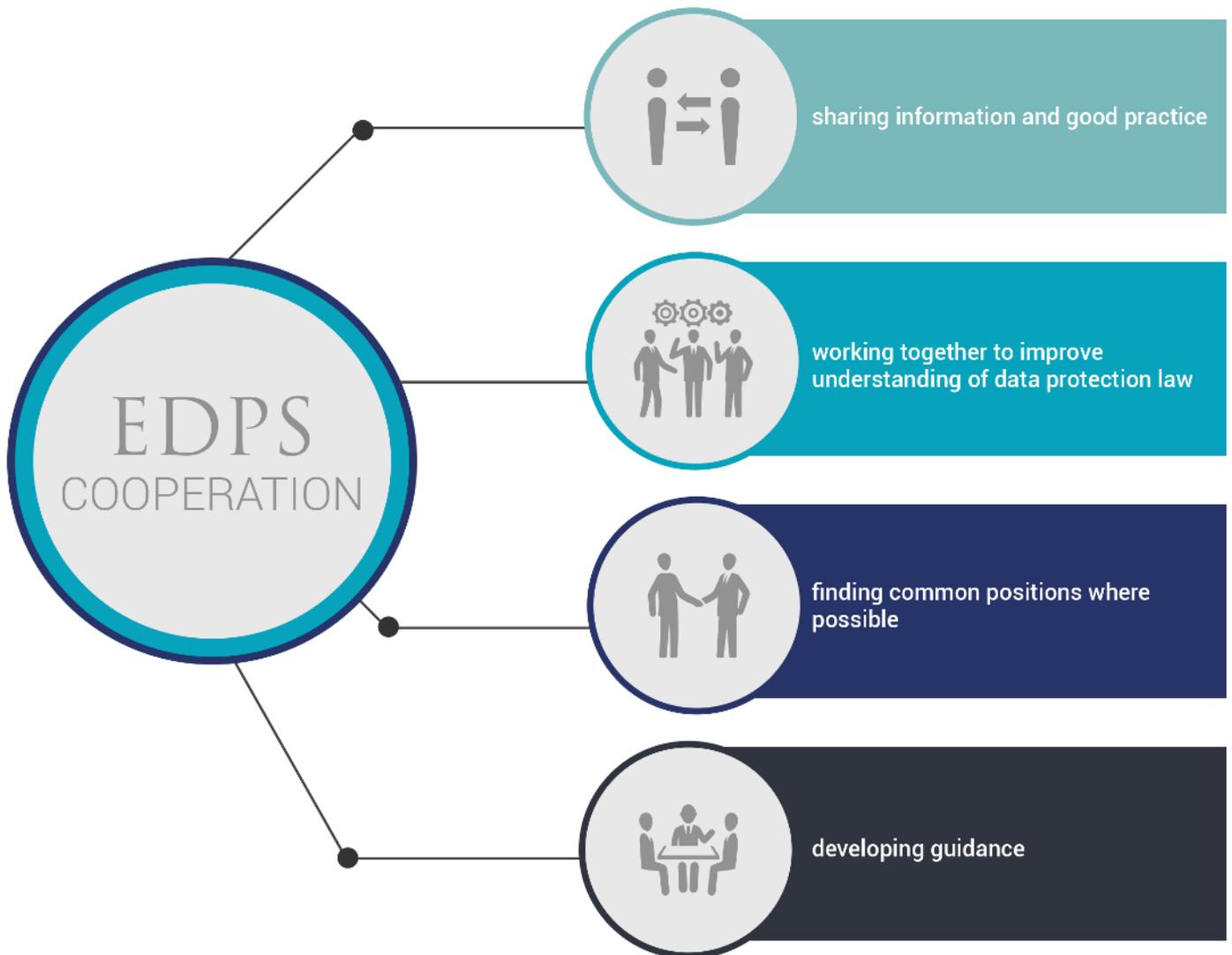
@EU\_EDPS

Glad [#EDPS](#) has strongly contributed to a balanced [@EU\\_EDPB](#) opinion of paramount importance on the first [#GDPR](#) adequacy finding: Not a red light, but improvements are recommended to achieve a robust [#EU](#) & [#Japan](#) [#dataprotection](#) deal

#### 4.5.2 International cooperation

##### Council of Europe

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data was the first legally binding international instrument in the field of data protection. Adopted by the Council of Europe on 28 January 1981, any country can sign up to what is known as Convention 108.



53 countries are now party to the Convention and its additional Protocol regarding supervisory authorities and transborder data flows. These include Cape Verde and Mexico, where the Convention entered into force on 1 October 2018. When combined with the number of countries participating in the Committee of Convention 108 as observers, this number increases to 70 countries, all working together on privacy and data protection rights.

The role of the EDPS, as an EU institution, is to act as an observer in the Council of Europe’s expert groups on data protection. These groups include the Consultative Committee (T-PD) of Convention 108. We attend the meetings of the expert groups and provide comments, with a view to ensuring both a high standard of data protection and compatibility with EU data protection standards.

For some time now, the Council of Europe has been working to modernise Convention 108. The aim was to strengthen its effectiveness and ensure that it better reflected the realities of an increasingly connected world. The EDPS has followed this process throughout.

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. Known as **Convention 108+**, the new Modernised Convention 108 was opened for signature on 10 October 2018 and signed by 21 states at an official ceremony.

In 2018, we contributed to the T-PD’s discussions on a recommendation on health-related data, ongoing work on the follow-up mechanism of Convention 108+, Artificial Intelligence (AI), the Internet Corporation for

Assigned Names and Numbers (ICANN) and on law enforcement transborder access to data.

### International Organisations

Though they may be exempt from national laws, including those relating to data protection, international organisations are influential advocates for the development of a privacy culture. Their position means that they are able to spread knowledge about data protection and privacy in parts of the world where, for various reasons, it has not necessarily been high on the agenda.

We support international organisations in their efforts to develop their own data protection frameworks and to share knowledge and experience with one another. An important part of this work takes place as part of a series of workshops, an initiative we launched in 2005.

In July 2018, Assistant Supervisor Wojciech Wiewiórowski participated in the seventh edition of these workshops, which we had the pleasure of co-organising in Copenhagen alongside our hosts, the Office of the United Nations High Commissioner for Refugees.

The workshop focused on a range of topics. These included:

- privacy standards and oversight mechanisms for international organisations;
- how to put the principle of accountability into practice;
- international transfers;
- the legal grounds for processing personal data in the international organisations context.

Throughout our discussions we noted a common determination to make data protection part of the working culture of international organisations and to ensure that these organisations are held accountable. We have no doubt that the productive dialogues initiated at this workshop will lead to further collaboration between international organisations themselves as they continue to develop their approaches to data protection. The EDPS will lend our full support to this effort.

### The Berlin Group

The EDPS has been an active member of the International Working Group on Data Protection and Telecommunications (IWGDPT, known as the Berlin Group) since its establishment. The group's work is

becoming more important with the increasing emphasis placed on the role of technology and its impact on fundamental rights, as well as the legal recognition of data protection by design as an obligation for controllers.

As a global cooperation body, the IWGDPT brings together actors from different parts of the world, not only from both sides of the Atlantic, but also from beyond the Pacific. All have different views and approaches to the rights of individuals and the models for their protection. Finding a common position reconciling the various backgrounds can be challenging, but this makes the results even more powerful and worthwhile.

IWGDPT Working Papers are based on an analysis of the technological features involved in the subject of the paper. They then proceed to define principles and recommendations aimed at achieving common objectives. In 2018, Working Papers concerned data processing and collection in connected vehicles. The group also worked on the privacy challenges of Artificial Intelligence.

### The Ibero-American Conference

The sixteenth Ibero-American conference on data protection took place from 28-30 November 2018, in San Jose, Costa Rica. We had the privilege of attending the conference, which brought together representatives from South and Central American DPAs, big companies and civil society.

Among the topics discussed were relations between the EU and Latin America, the protection of the personal data of minors, new perspectives in the processing of health data, security versus privacy and the role of civil society in the protection of personal data. The EDPS contributed to the panel on transparency and data protection.

A closed session took place on the last day, allowing authorities from participating countries to provide one another with an update on their legislation in the field of data protection, including amendments, the signing of international conventions and the drafting of new legislation. The conference was an excellent opportunity for us to develop relations with our counterparts in Latin America.

## 4.6 DIGITAL ETHICS

Over the past two decades, we have witnessed a digital revolution that has changed our world in ways that were previously unimaginable. While numerous developments have brought benefits, we also need to confront a range of new problems and challenges. Many of these are

linked to how data is collected and used in the age of digital technologies. To address this new reality, we committed to developing an ethical dimension to data protection in our [Strategy 2015-2019](#).

Our work on ethics starts with the question of how fundamental values and rights can be upheld in the digital age and aims to promote awareness and understanding of the risks we face. We want to assess how data protection and privacy are linked to preserving human dignity in the digitised world and explore their meaning and importance, taking into account extensive tracking and profiling practices, the Internet of Things, big data, Artificial Intelligence (AI) and autonomous systems, robotics and biometrics.

Ethics is about defining right and wrong, both in theory and in practice, in specific circumstances. While it is not an alternative to law, it informs laws as they are being drafted, interpreted and revised. It can also help guide people and organisations in deciding whether or not to act in an area where the law appears to be silent. The [EDPS Ethics Initiative](#) aims to reach out beyond the immediate community of EU officials, lawyers and IT specialists and generate a global conversation about this.

2018 was a pivotal year for the Ethics Initiative. The year began with the publication of the [Ethics Advisory Group Report](#) and ended with a week of intense and productive discussion during the [2018 International Conference of Data Protection and Privacy Commissioners](#). After more than three years of hard work, digital ethics is now very much on the global agenda. It is vital that we now work to capitalise on this and move the debate forward.

#### 4.6.1 The Ethics Advisory Group: Reporting on Digital Ethics

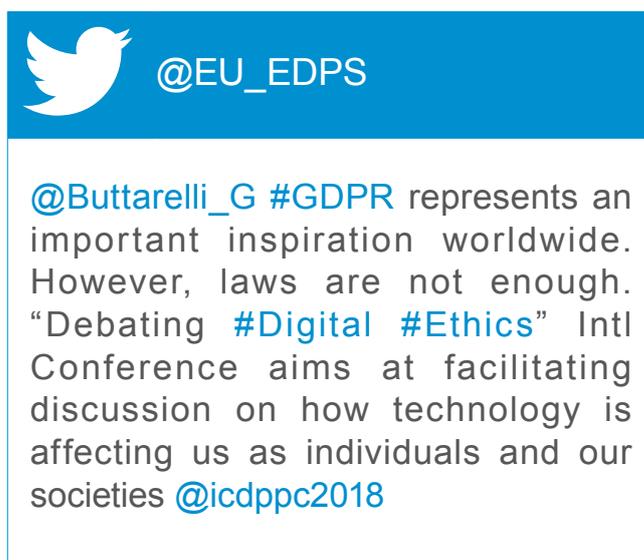
The [Ethics Advisory Group](#) (EAG) was launched by the EDPS at the annual Computers, Privacy and Data Protection (CPDP) conference in January 2016 as part of the EDPS Ethics Initiative. Made up of six experts with different backgrounds, its task was to explore the relationships between human rights, technology, markets and business models in the twenty-first century.

Over the course of two years, the group worked together to examine digital ethics from a variety of academic and professional perspectives with the aim of contributing to the wider debate on the digital environment and its ethical implications.

The EAG returned to the CPDP conference in 2018, as part of a panel organised by the EDPS, to present their [final report](#) and discuss the questions raised within it. The report focused on the consequences of the digital

revolution and the impact that these consequences have had on the values we, as individuals and as a society, hold dear. It identified the main socio-cultural shifts that have taken place in tandem with the latest technological developments, examining the relationship between them, human values and ethical agency, and addressed why this requires a reassessment of the data protection ecosystem.

The aim of the report was not to produce definitive answers or articulate new norms, but to encourage proactive reflection on what is at stake.



#### 4.6.2 Getting your views on Digital Ethics

On 15 June 2018, we launched a public consultation on digital ethics. The aim of the consultation was to build on the results of the EAG report, opening up the debate to contributions from individuals and organisations across all sections of society. In particular, we wanted to better understand how they were affected by the shift to digital, the specific challenges they were facing and to what extent they were addressing these challenges using an ethics-based approach.

We received 76 responses to the consultation, from a wide variety of sources located all over the world. These included health centres, kindergartens, universities, governments, NGOs, law firms and software developers, among others. The consultation consisted of 12 questions, the majority of which invited open answers, allowing us to collect vital qualitative information. From these answers we were able to reach one main conclusion: ethics was on the agenda of the majority of the organisations who participated in the consultation and was considered to be extremely relevant.



Contributors cited examples of some of the challenges we face and need to address. These included robots in healthcare and personal digital assistants, online voting, state nudging and the future of work. One contributor commented that *privacy goes beyond compliance, mastering the privacy challenge enables sustainable digital opportunities*. Another noted the importance of *human rights and European values of liberty, equality, freedom, democracy*, while a third acknowledged that *the challenges are immense and difficult*.

The results of the consultation were published on 25 September 2018 as part of a [short summary](#).

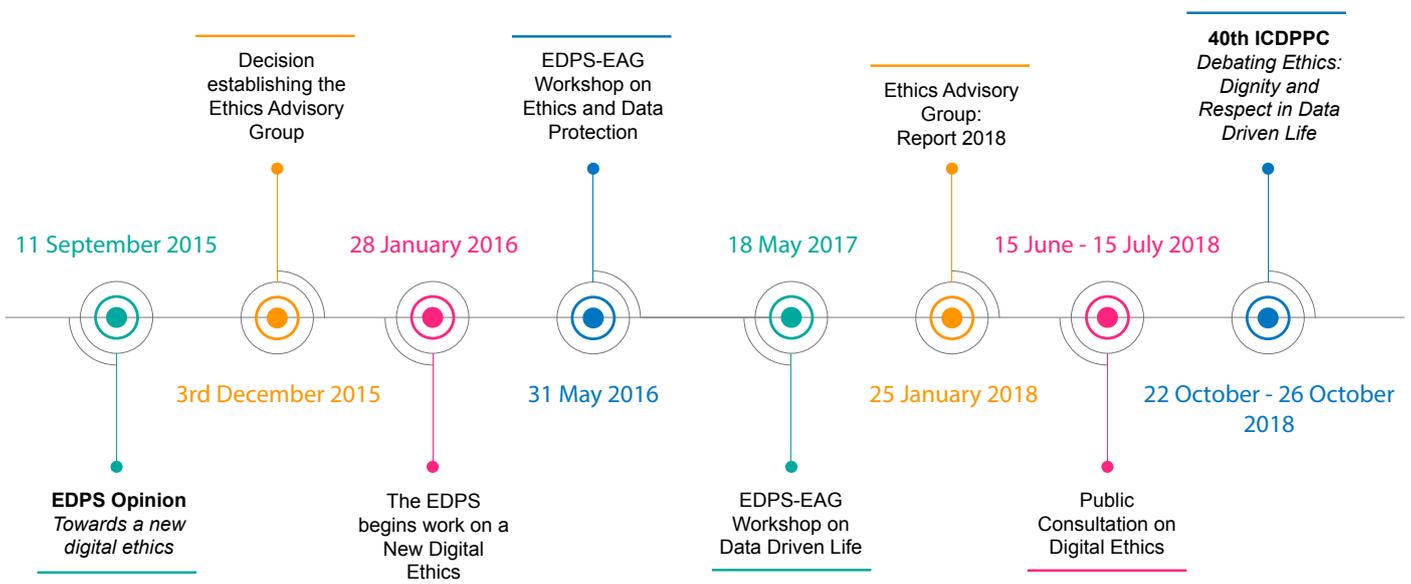
### 4.6.3 Encouraging debate around the world

From 22-25 October 2018, more than 1000 people, representing a wide range of disciplines, nationalities and viewpoints, descended on the European Parliament in Brussels to debate digital ethics (see [section 4.7](#)). The 40th International Conference of Data Protection and Privacy Commissioners proved to be a watershed moment for the debate on digital ethics, building on the work produced through the EDPS Ethics Initiative to incite a global reaction to the challenges we face in the digital age.

While new laws, such as the GDPR, provide us with a comprehensive framework for data protection in the digital age, they are only a first step in ensuring that we are able to reap the benefits offered by new technologies, while still enjoying our fundamental rights.

We dedicated the conference to *Debating Ethics: Dignity and Respect in Data Driven Life*. Ethical deliberation is the process of societal self-reflection, upon which members of a society establish values and norms and enact legal systems. Simply put, ethics come before, during and after the law, helping us to ensure that our laws remain up to date. History has shown that ethical notions of good and bad must be debated and defined on a continuous basis, by means of open and democratic discussion. Ethics, therefore,

## The EDPS Ethics Initiative: Three Years in the Making



can help us to find a path into an increasingly digital future that both reaffirms and protects long-standing rights and values.

The challenges posed by the digital revolution require a global response. Through the conference, we were able to generate the rich global and cross-disciplinary debate that can inspire this. Speakers included high-level EU representatives, renowned academics, pioneers of the online world, refuseniks, activists, human rights defenders and NGO representatives, Silicon Valley VIPs, legal experts, writers and journalists, thinkers and dreamers and, of course, representatives from data protection authorities from all over the world.

Through our communication efforts, the diverse issues raised at the conference reached a huge number of people, raising awareness and sparking reaction all over the world. With at least 1500 online articles published during the week of the conference, in addition to other media coverage, we were able to reach far beyond the 1400 people who attended the conference. This undoubtedly helped us to mobilise a wide range of people, beyond the data protection community and beyond Europe, and to make great strides towards our common goal of developing an ethical dimension to data protection.

A [full report](#) on the outcomes of the conference is available on the EDPS website ([see section 4.7](#)). In addition to this, as part of our continued work on the EDPS Ethics Initiative we will produce a new EDPS Ethics Opinion in 2019.

## 4.7 THE 2018 INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS

In 2018, the EDPS had the privilege of hosting the 40th International Conference of Data Protection and Privacy Commissioners, alongside our co-hosts, the Bulgarian Commission for Personal Data Protection (CPDP). This was the first time that this annual conference, which took place from 22 to 26 October 2018, had been held by an EU institution in collaboration with a national supervisory authority.

The Conference began with a two-day closed session, open only to conference accredited members. We then welcomed participants from all over the world to the public session of the Conference. Participants included representatives from government, civil society, regulators, industry, academics and the media, in

addition to [data protection authorities](#) (DPAs). Forty side events on a wide range of privacy related issues also took place and additional privacy events were also organised by our co-host in Sofia.

The 40th International Conference of Data Protection and Privacy Commissioners was an event unlike any of its predecessors. It did not focus on privacy or data protection or specific laws like the General Data Protection Regulation (GDPR), or even on laws in general. Rather, through *Debating Ethics: Dignity and Respect in Data Driven Life*, we aimed to build on the work started by the [EDPS Ethics Initiative](#) and stimulate an honest and informed discussion about how we should shape the impact of digital technology on individuals and societies. As a result of our efforts in this area, the EDPS is now viewed as a leading authority on digital ethics.

A [detailed report](#) on the Conference can be found on the EDPS website.



### 4.7.1 The Closed Session - Ethics and Artificial Intelligence

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) is a recognised international organisation. Throughout its 40 year history, the conference has met each year, bringing together DPAs from local, national and international levels to share knowledge and provide support.

The ICDPPC Executive Committee sets the agenda for the closed session. In 2018, for the first time, the central theme of the closed session was directly connected to the theme of the public session.

The closed session of the International Conference is open only to accredited members and observers of the [ICDPPC](#). Bringing together a record number of 206 delegates from 76 countries, it took place at the

prestigious Palais d'Egmont, in Brussels, from 22-23 October 2018. Ethics and Artificial Intelligence (AI) was this year's topic of discussion.

Few authorities currently monitor the impact of new technologies on fundamental rights so closely and intensively as data protection and privacy commissioners. The 2018 conference continued the discussion on AI initiated two years previously at the conference in Marrakesh, which was based on a [reflection paper](#) produced by the EDPS.

Our discussions resulted in a [declaration](#) on ethics and data protection in artificial intelligence, spelling out six principles for the future development and use of AI and demanding concerted international efforts to implement these principles. Conference members will contribute to these efforts in different ways including through a [public consultation](#) and a new permanent working group on Ethics and Data Protection in Artificial Intelligence.

The closed session also adopted three other resolutions on [e-learning platforms](#), on the [Conference Census](#) and on [collaboration between Data Protection Authorities and Consumer Protection Authorities](#), in addition to a [roadmap for the future of the International Conference](#).

We hope that the decisions taken in the closed session help the conference to grow in ways that will reinforce cooperation globally. As a community of regulators, the ICDPPC must now look to interact much more with partners from outside the world of data protection.

#### 4.7.2 The Public Session - Debating Ethics



The public session of the 2018 International Conference took place from 24-25 October 2018, in the Hemicycle of the European Parliament in Brussels. In addition to guests, members and observers of the ICDPPC, we

welcomed participants from diverse backgrounds and nationalities. These included representatives from the private and public sectors, academia, civil society and the media.

With the choice of topic for the public session at the discretion of the hosts, we chose to focus on *Debating Ethics: Dignity and Respect in Data Driven Life*. We wanted to inspire an inclusive, cross-disciplinary and interactive debate on the digital revolution and its impact on us, as individuals and as a society (see [section 4.6](#)).

Split into five sessions across two days, the conference drew on contributions from a diverse group of speakers. These included high-level EU representatives, renowned academics, pioneers of the online world, refuseniks, activists, human rights defenders and NGO representatives, Silicon Valley VIPs, legal experts, writers and journalists, thinkers and dreamers and, of course, representatives from DPAs from all over the world.



@EU\_EDPS

[#EDPS](#) [@Buttarelli\\_G](#) opens the 2018 Olympic Games on [#Privacy](#) - "Choose humanity: putting the dignity back into digital". The 40th International Conference will explore the human dimension of new technologies. [#DebatingEthics](#) [@icdppc2018](#)

#### Session one - This Digital Life

The conference began with a discussion of the role of ethics in human society. Maria Farrell, a writer and consultant on technology, internet policy and community, began the conference with a call for collective action that set the tone for the discussions to come.

EDPS and host, Giovanni Buttarelli, officially opened the conference, setting out the strategic importance of defining a truly global digital ethics that safeguards dignity and respect for individuals and groups in the decades to come. Integral to this is the need for an objective assessment of how technologies are affecting our lives and how we can ensure a positive relationship

with new technologies, which puts people and dignity at the centre.

He finished his speech by welcoming one of our keynote speakers, Tim Cook, to the stage. In a much-anticipated address, the Apple CEO made a powerful call for the development of a digital ethics and acknowledged the responsibility of Apple and other powerful developers in ensuring technology serves humankind.

### Session two - Right versus Wrong

The second session looked to assess how the latest technological innovations impact our privacy, autonomy and self-determination. We wanted to explore how ethics interacts with the law, the role it has played in other fields and the role it plays in resolving public policy dilemmas.

Inventor of the World Wide Web Sir Tim Berners-Lee and Professor of Law and Philosophy at the University of Pennsylvania Anita Allen opened the discussion. While the former highlighted the role of technological development in shaping society, the latter encouraged us to view ethics as something which complements the law, rather than undermines it.

A panel discussion followed, featuring renowned ethicists and scholars who offered insights into the application of ethics in different fields.

### Session three - The Digital Dividend

In the last session of the day, we looked at the wider social consequences of ethics. The aim was to explore the effect of new technology on the values and rights at stake for individuals and human interaction, society and the state

The CEOs of two of the world's biggest technology companies, Facebook and Google, contributed to our discussion through video messages, while Former Chief Justice of India, Jagdish Singh Khehar, provided us with a real-life example of how ethics can be enforced.

After a panel discussion on the impact of emerging technologies on society and the economy, it fell to our co-host, Chairman of the Bulgarian Commission for Personal Data Protection Ventislav Karadjov, to summarise the day's discussions.

We ended the day with computer philosophy writer Jaron Lanier's call for a less manipulative alternative to the advertising business model which currently dominates the technology sector.

### Session four - Towards a Digital Ethics

EU Commissioner for Justice Vera Jourová opened our second day of discussions, which focused on the idea of *data protection beyond compliance*. We attempted to determine what this concept means, who should speak about it and who needs to take action.

An important question in this debate concerns the role of DPAs in the governance of digital ethics. A panel discussion featuring privacy commissioners from every continent, as well as esteemed experts from government, civil society and industry, attempted to address this question.



### Session five - Move Slower and Fix Things

Our final session aimed to draw conclusions from the preceding discussions, with a particular focus on how to move forward. It included a report on the outcomes of the Creative Café, a workshop session held in parallel to session four, which aimed to explore this question.

Speaking on behalf of the Creative Café, Assistant Supervisor Wojciech Wiewiórowski stressed the that the conference represented only the beginning of a much longer process.

EDPS Giovanni Buttarelli brought the conference to a close. He referenced the diversity of the voices heard throughout the sessions, from those who represented powerful interests, to those who spoke for the most disadvantaged, who are yet to truly benefit from the digital revolution.

Over 40 people took to the stage during the public session of the international conference, offering their

diverse perspectives on the subject of digital ethics. Common to all of their contributions was a promise: to continue the collaboration instigated by the conference in pursuit of a sustainable digital ethics.



### 4.7.3 Side Events

In the tradition of past years, side events once again took place in the margins of the 2018 international conference. These focused not only on the conference theme of digital ethics, but also on a wide range of other topics relating to data protection practice. With over 40 events to choose from, all taking place on 23 and 25 October 2018, there was something for all interests.

Organised by a variety of different organisations and groups from all over the world, the side events that took place during the week of the international conference week provided a unique opportunity for participants to interact with colleagues from diverse nationalities and backgrounds and to learn from their differing perspectives on a range of data protection issues. The diversity of topics discussed is well illustrated by a selection of events.

In the year of the [General Data Protection Regulation](#) (GDPR) it is perhaps unsurprising that many of our side events focused on the topic. The EDPS and the European Data Protection Board (EDPB) jointly hosted one such event on 25 October 2018. Experts from data protection and other authorities across the EU and globally joined the heads of the EDPS and EDPB, Giovanni Buttarelli and Andrea Jelinek, for a discussion on the GDPR, five months after it became fully applicable. The event was honoured to welcome Koen Lenaerts, President of the Court of Justice of the European Union, and Catherine De Bolle, Europol's Executive Director, as its keynote speakers.

Another event, organised by the Council of Europe, saw an impressive line up of data protection experts discuss their views on the modernisation of Convention 108, the world's only international treaty safeguarding the right to data protection ([see section 4.5.2](#)). The event aimed to unpack the newly updated Convention

108, providing information about the new text, its value and benefits.

Public Voice Coalition, a broad coalition of civil society organisations, organised another event, focused on one of the hot topics in data protection at the moment: Artificial Intelligence. With clear connections to digital ethics, the event looked to explore the implications of AI for human rights, consumer protection and competition and the relationship between ethics and the law.

Side events were organised by eight different DPAs from around the globe, 18 NGOs and international organisations, six think tanks and research groups and eight private companies and law firms. Over 160 speakers were involved in what proved to be a very diverse selection of events.



### 4.7.4 Social Events

In order to offer a unique experience for delegates coming to Brussels from all around the world, we secured some of Brussels' most striking and prestigious venues to host the conference. We wanted to give delegates a taste of what the *Capital of Europe* has to offer, including its impressive history and architecture.

The week started at Brussels' Hôtel de Ville, an impressive Gothic building dating back to the fifteenth century. Delegates from over 80 countries were greeted with a Welcome Cocktail and a spectacular view of Brussels' central square, the Grand Place.

From 22-23 October 2018, ICDPPC accredited members and observers gathered at the Palais d'Egmont, the venue for the closed session of the conference. Originally constructed in the sixteenth century, the Palais d'Egmont has played host to several members of the European royalty and nobility over the years, including Queen

Christina of Sweden and Louis XV, as well as to prominent European philosophers and artists, such as Voltaire and Jean-Baptiste Rousseau. Now the property of the Belgian Ministry of Foreign Affairs, it hosts a range of important diplomatic events and has welcomed some of the world's most influential and well-known heads of state.

The venue for the public session was equally impressive. The Hemicycle of the European Parliament usually hosts the world's largest transnational parliament. From 24-25 October 2018, however, it played host to a debate between over 1000 people on the impact of the digital revolution.

Evening events were planned with the same attention to detail. The first day of discussions in the closed session concluded with dinner at the Concert Noble. This historic manor was built by King Leopold II in the nineteenth century to provide an appropriate backdrop for gatherings of aristocratic socialites to enjoy music and art.

A Welcome Cocktail was organised on 23 October 2018 at the inspiring Museum of Fine Arts, in Brussels' Place Royale. The theme for the event was *An Evening in Brussels* and it was organised by the conference hosts in conjunction with the International Association of Privacy Professionals (IAPP). Taking place on the eve of the public session, it included a tour of the works of the famous surrealist painter René Magritte, as well as the chance to sample some typical Belgian beers from local breweries and the world-famous Belgian chocolate.

Following an intense first day of debate on digital ethics, we organised the traditional Gala Dinner, which took place at the spectacular Autoworld Museum. The museum is home to one of the biggest vehicle collections in the world and the event proved an excellent opportunity for networking.

As no visit to Brussels is complete without a visit to the Atomium, the final event of the week was organised in this atom-shaped museum, in collaboration with The Floop and Qwant. This Brussels landmark was originally constructed for the 1958 World Expo in Brussels.



#### 4.7.5 Conference Communication

Encouraging debate on digital ethics around the world is one of the main aims of the Ethics Initiative, as outlined in the [EDPS Strategy](#) (see section 4.6.3). With this in mind, we put in place a comprehensive media strategy aimed at ensuring broad, international coverage of the conference, that would incite global debate.

We also wanted to ensure the participation of all those attending the conference. We therefore invited every participant to get involved in the conference discussion, most notably through our conference app.

##### Media campaign

Eighty-one media organisations from 23 different countries and all continents followed the four-day event, totalling 125 journalists. Broadcasters, news agencies and leading newspapers were all in attendance, including media outlets such as CNN, CNBC, Bloomberg, The Wall Street Journal and the Financial Times. While the most highly-represented nations were Belgium, the United States, Italy and the United Kingdom, we also welcomed journalists from Japan, China, the United Arab Emirates, Senegal, Kenya and elsewhere. Press coverage of the conference was truly global in scope.

This international media presence reflected global interest in both the topic of discussion and the speakers involved. Keynote speeches from Apple CEO Tim Cook and inventor of the World Wide Web Sir Tim Berners-Lee undoubtedly contributed to press interest in the conference and helped spread our message to a broader audience.

On 24 October 2018, the first day of the public session, we organised a press conference. Held in the European Parliament, it presented media professionals with an opportunity to directly address some of our speakers, including EDPS Giovanni Buttarelli, Sir Tim Berners Lee and UK Information Commissioner Elizabeth Denham, among others. We also published a press release.

Press coverage of the conference well exceeded our expectations, with over 1500 online articles published between 22 and 26 October 2018.

##### The website

A dedicated [website for the international conference](#) was launched on 19 March 2018. Our objective was to create a user-friendly website where people could easily find out more information about the conference theme, programme, speakers and venues. It provided

for conference registration and offered participants the option to book a hotel through the website and contact us if they had any questions. ICDPPC members also had access to all meeting documents using their login details and password.

The website was available in two languages, English and French, and was updated regularly in both languages. Feedback received about the website was overwhelmingly positive and indicated that people were easily able to find the information they needed.

Throughout the conference, we aimed to keep the website up to date by promptly uploading documents, videos and news as soon as they were available to us.



### Social media

To encourage participants and others to get involved in the wider online debate both before and during the conference, we launched dedicated [Twitter](#) and [Instagram](#) accounts. We were active on both of these

channels, providing regular updates, information and coverage of the conference. We supported our activities on these channels using the EDPS social media accounts ([see section 7.1.1](#)).

We tweeted 128 times and our followers doubled over the course of the conference week. Our posts were retweeted over 1100 times and received 1400 likes. On Instagram, we posted 46 times and received 856 likes.

In parallel, the visibility of the EDPS Twitter, LinkedIn and YouTube accounts increased as a result of our efforts during the conference, allowing us to reach new people and significantly increase the impact of our social media accounts.

Our success on social media demonstrates both our increasing global influence as an authority on data protection and digital ethics and our ability to reach a wider audience.

### The app

To encourage audience participation in the conference, we developed and launched a free conference app, which was available to download from 3 October 2018. The app reflected and complemented the website. All delegates were encouraged to download it for use during the public session of the 2018 international conference.

Participants could use the app to take notes, take part in polls, share their views and send questions to the host for speakers to answer on stage. 965 people downloaded the app and more than 50% connected to their personal account.

## | 5. Court Cases



The EDPS can be involved in cases before the Court of Justice of the European Union (CJEU) in any of three ways:

- the EDPS can refer a matter to the Court;
- EDPS decisions can be challenged before the Court;
- the EDPS can intervene in cases relevant to our tasks.

We followed closely all court cases relating to the protection of personal data in 2018, though we were not directly involved in any ourselves. The rulings made on cases relating to data protection help us to interpret data protection law and to ensure that the fundamental right to privacy and data protection is fully respected.

## 6. Transparency and Access to Documents



As an EU institution and according to our Rules of Procedure, the EDPS is subject to Regulation 1049/2001, on public access to documents. Within the EDPS, the person responsible for handling these requests is a designated legal officer. In their role as

Transparency Officer, they collaborate with the relevant staff members in order to respond appropriately to the request.

In 2018, we received only nine public access requests for documents held by the EDPS, in comparison to the 11 requests we received in 2017. This decrease reflects the trend of the past few years. Of these requests, one case was reviewed at a confirmatory stage. In all cases the requested documents were either fully or partially disclosed.

It seems that the decrease in the number of requests received is the result of our proactive efforts to regularly update and publish information on our website in a simple and accessible way. 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.

# | 7. The Secretariat

## 7.1 INFORMATION AND COMMUNICATION

As the profile of data protection continues to grow, it is the job of the EDPS Information and Communication team to ensure that our messages and activities reflect and support the reputation of the EDPS as a leading authority in this area. This role is set out in the [EDPS Strategy 2015-2019](#), which commits the EDPS to making technical issues more accessible for non-experts and to communicating in a transparent manner, appropriate for the relevant audiences.

2018 was a particularly busy year for the communications team, and the EDPS in general. Preparations for the European Data Protection Board (EDPB) and the [General Data Protection Regulation \(GDPR\)](#) came to a head in May 2018, while we also launched and executed communications campaigns on the [2018 International Conference of Data Protection and Privacy Commissioners](#) (see section 4.7.5) and the new data protection rules for the EU institutions and bodies.

In addition to these activities, we continued our efforts to improve our established communication channels, building on the success of rebranding efforts over the past few years to reinforce the image of the EDPS as a respected global leader in the data protection field.

### 7.1.1 Online media



### Website

Since the launch of our new [website](#) in 2017, we have continued to make improvements by adding new features and improving the design. These efforts are aimed at providing the best user experience possible and ensuring that all visitors to the website are easily able to find the information they need.

One of the improvements we introduced in 2018 was to add a *Quick Links* section to the homepage to provide users with a shortcut to some of the most frequently used pages on our website. Where possible, we have also moved from publishing documents in PDF format to producing them in HTML, ensuring an improved user experience on mobile phones and tablets. In the interest of transparency, we ensure that the Supervisors' agenda is always up-to-date and clearly visible on our homepage and we regularly update our News section with important information on our work.

During the course of the year, we changed our approach to gathering statistics on the EDPS website. For this reason, we are unable to accurately report on the number of visitors to the EDPS website in 2018. Our new approach, however, is designed to ensure that the EDPS website is as data protection friendly as possible, by moving from *opt-out* tracking to an *opt-in* process.

Under the *opt-out* system, visitors to the EDPS website could follow the simple instructions provided in our cookie banner to opt out of having their activity on our website tracked. The new *opt-in* process, however, will ensure that we are only able to track visitors to our website if they explicitly provide us with consent to do so. The new system will be launched in January 2019. Until then, no tracking of any kind will take place on the EDPS website.

### Social Media

Social media has become indispensable as a communications tool. With our presence on three influential social media channels now well established, we are able to use these tools to quickly and easily reach a global audience.

While Twitter (@EU\_EDPS) remains our most influential social media tool, our presence on LinkedIn is growing rapidly and is now also a hugely influential tool for our communications activities. In addition to this, our communication efforts during the 2018 International Conference of Data Protection and Privacy Commissioners led to a significant increase in the number of followers on the EDPS YouTube channel, which we will look to build on over the coming months.

Our continued growth on social media is testament to our increasing global influence as an organisation, as well as our efforts to implement an effective social media strategy. This allows us to reach an increasingly diverse and global audience.



### EDPS blog

We launched the [EDPS blog](#) back in April 2016. Since then, the blog has gone from strength to strength. It is a platform through which the EDPS and Assistant Supervisor are able to communicate on a more personal level about their thoughts, opinions and activities, as well as the work of the institution in general. The blog is easily found on the homepage of the website where a short extract from the most recent blogpost is always displayed.

In 2018 we published 14 blogposts on a range of different subjects. These included the 2018 International Conference, ePrivacy, the EDPS meetings with [Data Protection Officers](#) (DPOs) and the new Regulation for the EU institutions and bodies. All of our blogposts were promoted through our social media channels and many of them also received media attention.

### 7.1.2 Events and publications


@EU\_EDPS

The key word of [#GDPRforEUI](#) is [#accountability](#). It means that personal data protection should be embedded in culture of organizations. Comply with [#dataprotection](#) law & demonstrate your compliance! Read our factsheet <https://europa.eu/!PY43hU> & watch video <https://europa.eu/!MM88bY>

#### The GDPR for EUI: the communication campaign

On 11 December 2018, the new data protection rules for the EU institutions and bodies became fully applicable. To complement our ongoing awareness-raising activities (see [section 4.1.2](#)), we launched a communication campaign. Though aimed principally at EU institution staff members, we also wanted to raise awareness among those outside the EU institutions about how the new rules might affect them and their rights.

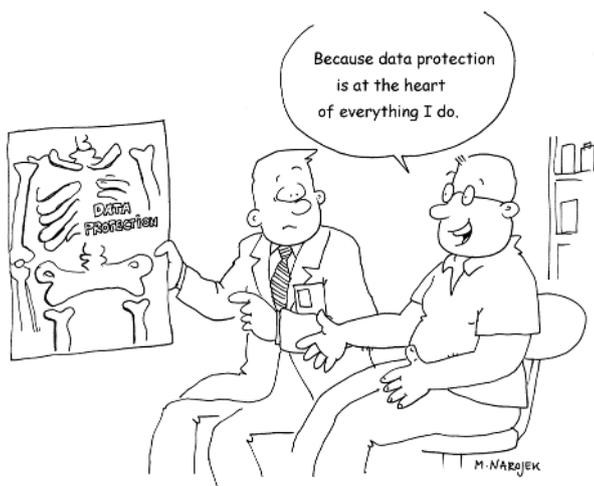
We put together a Communications Kit to raise awareness about the new rules within the EU institutions and provide relevant and helpful information for all EU staff members. This kit was distributed to all EU institution DPOs in advance of 11 December 2018, to help them reach out to staff members working in their respective institutions.

The kit included a [video on accountability](#), a poster for DPOs to print out and distribute in their buildings, artwork for use on their intranet or social media channels and webcam covers to be distributed among some EU staff members. It also included three factsheets, on [data protection rights under the new rules](#), [the implications of the new rules for EU employees](#) and on [ensuring accountability](#). Individual copies of the new rules were also prepared and distributed among DPOs at the EDPS-DPO meeting, which took place in Brussels on 12 December 2018 (see [section 4.4.1](#)).

To complement our collaboration with DPOs, we launched a press and social media campaign, aimed at raising awareness outside the EU institutions. This included using Twitter and LinkedIn to provide

information about the new rules, their implications and the role and activities of the EDPS. In addition to issuing a [press release](#) on 11 December 2018, we contacted some media outlets directly to try and ensure coverage. An advertisement was also published in Politico on 13 December 2018, featuring an engaging cartoon.

Efforts were also made to bring our website and Wikipedia entry up-to-date, to reflect the changed legislation.



### EU Open Day 2018

In celebration of Europe Day, on 5 May 2018 the EU institutions opened their doors to all members of the public. The annual EU Open Day is an opportunity for the EU institutions to increase the transparency of their work and to educate people on the EU's activities. For the EDPS, it is a chance to increase general public awareness of our role and data protection in general.

This year, the EDPS stand was once again located in the European Commission's Berlaymont building. EDPS employees were on hand from 10am onwards to answer questions from visitors and encourage them to take part in our data protection quiz. Facial detection software, which attempts to define a person's gender, age and emotions, also proved popular and undoubtedly contributed to a record number of people participating in the quiz.

With public awareness about privacy and data protection at an all-time high, the increased interest in data protection and the work of the EDPS was both understandable and encouraging. We look forward to welcoming even more people to our stand in 2019.



@EU\_EDPS

#EUOpenDay 2018 has started. Come and visit us! Your privacy counts! #eudatap #ecberlaymont

### Data Protection Day 2018

On 28 January each year, EU institutions, agencies and bodies, as well as the member states of the Council of Europe, celebrate Data Protection Day. This day marks the anniversary of the Council of Europe's data protection convention, known as Convention 108, the first binding international law concerning individuals' rights to the protection of their personal data.

This year, to mark the occasion, the EDPS trainees held a lunchtime conference on 12 February 2018, focused on data protection issues relating to modern-day dating apps. The EDPS and Assistant Supervisor provided the opening and closing remarks at the conference, which included panels on topics such as:

- what personal data dating apps can process and how they use this data;
- the rights of individuals to request access to the data held on them;
- digital ethics in the context of dating apps;
- privacy by design;
- algorithms used to *match* app users.

Taking place just two days before Valentine's Day, the conference theme proved successful in raising awareness about the risks and rights associated with widely-used apps, as well as in encouraging young people to engage in the data protection and privacy debate. The conference was webstreamed live on our website, ensuring that it was also accessible to a wider audience.

### Newsletter

After the launch of our new-look version in mid-2017, the [EDPS Newsletter](#) is more popular than ever. The new format means that it is now more accessible and user-friendly on all digital platforms and by publishing

more frequently we are able to ensure that our readers are kept up to date on our latest activities.

In 2018, we published nine editions of the EDPS Newsletter. These included our January special edition, in which we highlighted some of our less high-profile activities from 2017, and our special International Conference edition in September. Our mailing list continues to grow, with 3907 people now subscribed to our monthly updates. This serves as a constant reminder of the importance and relevance of the Newsletter as a communications tool.

### 7.1.3 External relations

#### Media relations

We issued ten [press releases](#) and statements in 2018. This is comparable with our efforts in 2017 and demonstrates the consistency of our current media relations approach, which also draws on social media and the blog to generate media coverage. All of our press releases were published on the EDPS website, distributed to our network of journalists and other

interested parties and published on the EU Newsroom website.

We also received 104 formal requests from European and international press on a wide variety of topics.

Some of the topics on which we received significant press coverage during the year include the 2018 International Conference, the General Data Protection Regulation (GDPR) and fake news and the Cambridge Analytica/Facebook scandal. Media coverage was particularly notable in Italy, the home country of the EDPS, Giovanni Buttarelli.

#### Study visits

In 2018, we hosted 12 study visits to the EDPS. As the profile of data protection has increased, so has interest in our work. Though we would like to host every group that expresses an interest in the EDPS and what we are doing, with the high workload we faced in 2018 and the limited space available to host these visits, we were unfortunately forced to be a bit more selective.

## EDPS Information & Communication in 2018: the statistics



#### Online media:

14 024 Followers on Twitter  
475 EDPS tweets  
9169 Followers on LinkedIn  
1250 Followers on YouTube

#### Events and publications:

3907 Newsletter subscribers  
14 Blogposts

#### External relations:

10 Press releases  
104 Formal requests from press  
12 Study visits  
516 Public information requests

Nevertheless, study visits comprise an important part of our communications strategy, allowing us to communicate directly with students, legal experts, privacy professionals and other influential groups to raise awareness about the work of the EDPS and the EU on data protection and privacy.

### Information requests

The number of public requests for information received by the EDPS has been growing year on year, and 2018 was no exception. In fact, in 2018 we witnessed an enormous increase in requests. As in past years, the majority of these requests related to matters over which the EDPS has no competence.

One reason for such a significant increase in requests was the introduction of the GDPR in May 2018. We received a large number of requests relating to the implementation of these new rules, although we were not the relevant competent authority to answer them. The increased visibility of the EDPS, both as a result of the heightened profile of data protection and of our activities relating to the 2018 International Conference, also helps to explain this increase.

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.

#### 7.1.4 The EDPB

Preparations for the EDPB began well in advance of 25 May 2018 (see section 4.1.1), when the Board officially started its work as an EU body. Though the Board itself has its own communications team, the EDPS Information and Communication team acts in a support role, as and where required.

In the lead up to May 2018, the majority of this work focused on ensuring that the EDPB would be ready to start work from day one. To do so, they needed a website. We worked closely with colleagues from the EDPB to ensure that their website was ready and fully functional in time for the launch of the EDPB on 25 May 2018, also ensuring that EDPB staff members received training on how to use the website.

In addition to this, we provided a lot of graphic support, helping to design and produce publications and other graphic materials in line with the corporate identity of the EDPB.

Since the launch of the EDPB, we have continued to support their communications team in their activities and also participate in regular conference calls organised by the EDPB secretariat with communications representatives from the other EU [data protection authorities](#) (DPAs) which make up the EDPB. We hope that this productive relationship will continue.

## 7.2 ADMINISTRATION, BUDGET AND STAFF

The role of the Human Resources, Budget and Administration (HRBA) Unit is to provide support to the EDPS Management Board and operational teams and help them to achieve the goals set out in the [EDPS Strategy 2015-2019](#).

The Unit carries out traditional HR tasks, but is also responsible for careful management of the institution's budget and the implementation of new policies, which ensure that working life at the EDPS runs smoothly.

2018 was a busy year for the HRBA Unit and the EDPS in general. Among many other things, we welcomed the European Data Protection Board (EDPB) secretariat, launched a data protection competition to help us recruit new staff members, completed our preparations for the new data protection Regulation for the EU institutions and introduced some new HR initiatives.

### 7.2.1 Budget and finance

#### Budget

In 2018, the EDPS was allocated a budget of EUR 14 449 068. This represented an increase of 27.59% in comparison with the 2017 budget.

As in previous estimates, our budgetary proposal made a clear distinction between so-called current and new activities. For the current activities, we persisted with the policy of austerity recommended by the European Commission. Most budget lines therefore remained frozen at 0%, with an overall increase of 1.54%. This increase was lower than the predicted cost of living at the time of 1.8%, which was the ceiling proposed by the Commission.

With regard to new activities, the budget increase of 27.59% came mainly as a result of the establishment of the new EDPB. This covered our request for six additional full time employees, as well as the budget required for the Board's operation and activities, which began on 25 May 2018.

The expected budget implementation rate for 2018 will be around 94%. This is quite high given the uncertainties related with establishing a new body such as the EDPB, and the budgetary impact this could have.

## Finance

For the seventh consecutive year, the Statement of Assurance of the European Court of Auditors concerning the financial year 2017 (DAS 2017) did not contain any observations concerning the reliability of our annual accounts.



## Procurement

In 2018, we began work on a new initiative named the *Procurement Professionalisation Project*. We will implement the new project over the course of 2019. It has three main objectives:

- the appointment of specific Operational Initiating Agents in each operational unit and sector of the EDPS, who will receive specific training on procurement procedures;
- the implementation of a paperless, electronic workflow;
- a review of existing procurement procedures with the aim of improving our efficiency and simplifying the current procedures.

In 2018 we awarded three calls for tender with a value of over 15.000 EUR. These were:

- CAMERON - Media training (60 000.00 EUR)
- FORUM EUROPE - Organisation of the ICDPPC - Conference 2018 (134 900.00 EUR)
- WEBER SHANDWICK - Communication agency (144 000.00 EUR)

Some major projects and contracts were also concluded through inter-institutional framework contracts. These were:

- **DIGIT/DI-07360-00 (SIDE)/European Commission**
  1. The renewal of our Case Management System (CMS), VDE/SAAS and Consultancy Services (Fabasoft)
  2. Online media monitoring and international media database (Meltwater)
- **ITS14 (Lot 2 and 3)/European Parliament**
  1. Web Developers and Drupal Developers for the EDPS, EDPB and 2018 International Conference websites
  2. IT Analyst and Development Specialist for the analysis and development of IT Tools

### 7.2.2 Preparing for the EDPB secretariat

The EDPB is an independent body, the secretariat of which is provided by the EDPS. While the secretariat itself is responsible for providing the Board with administrative, logistical and analytical support, we are responsible for ensuring that the EDPB receives adequate human and financial resources and for providing administrative support where needed ([see section 4.1.1](#)).

In March 2018 we welcomed the new EDPB secretariat to the first floor of the EDPS offices. However, many other administrative and logistical tasks also had to be completed before the EDPB officially began its work as an EU body on 25 May 2018.

#### Internal decisions

The EDPB started work on the same day that the new [General Data Protection Regulation](#) (GDPR) became fully enforceable. It was therefore essential to ensure that, as from 25 May 2018, all staff members transferred from the EDPS to the EDPB, as well as any new EDPB staff members, would still benefit from the same rights and be subject to the same rules as those working for the EDPS.

We therefore carried out a review of all existing decisions, guidelines and manuals and a general decision was signed by the EDPS Director. While some specific decisions still need to be updated to take into account particularities relating to the EDPB secretariat, the majority of the work has now been completed.

### Updating service-level agreements

The EDPS has several service-level agreements (SLAs) with external providers which help individual staff members and the EDPS in general to perform their roles effectively and efficiently.

All SLAs which cover EDPS staff members apply automatically to staff members of the EDPB secretariat. However, some SLAs refer only to the provision of services. These needed to be updated to ensure that EDPB staff members could make use of these services.

During the first half of the year, several SLAs were therefore updated to include the EDPB. In other cases, new SLAs were signed directly between the EDPB secretariat and the service provider. This helped us to ensure business continuity and a smooth start for the EDPB secretariat.

### A pilot programme for short secondments

The 28 EU [data protection authorities](#) (DPAs) and the EDPS make up the EDPB. Strong cooperation between all of these members is essential to achieving results. To be truly effective, this cooperation should extend beyond data protection experts, to human resources experts as well.

On 29 September 2018, we organised a meeting between the HR units of the EU DPAs to discuss a pilot programme of EDPB short secondments. We wanted to discuss the idea and exchange proposals, in order to develop a programme which could be of benefit to all DPAs.

The programme will provide a pool of experts in different areas willing to visit another DPA or the EDPB secretariat and exchange knowledge. We hope to launch the pilot programme at the beginning of 2019.

### 7.2.3 A competition for data protection specialists

To cover the recruitment needs of both the EDPS and the EDPB, we asked the European Personnel Selection Office (EPSO) to launch a new open competition for 30 Administrators in the field of data protection.

Both the EDPS and the EDPB have an increasing need for expert staff, not only to cover the usual staff turnover, but to help both organisations to fulfil their roles and responsibilities effectively. While the EDPB is a new and growing EU body, the EDPS must take on new staff to complete additional tasks assigned to us by the EU legislator, such as the supervision of Eurojust (see [section 4.4.13](#)). There is therefore a clear need for

a pool of highly qualified data protection experts to satisfy our future recruitment needs.

This is the second data protection competition organised by the EDPS since 2015. We expect the new reserve list of candidates to be ready by mid-2019.

### 7.2.4 The GDPR for EU: HR preparations

As an EU institution, the EDPS is not only responsible for supervising and enforcing the new data protection rules within the other EU institutions and bodies, we must also apply them to our own work and try to set an example for other institutions to follow (see [sections 4.1.2 and 8.2](#)).

The new Regulation affects numerous HR decisions. We therefore initiated a full review of our HR data processing activities. Working in close cooperation with the EDPS Supervision and Enforcement Unit, [Data Protection Officer](#) (DPO) and Assistant DPO, we drafted new data protection records and revised our data protection notices in order to ensure that we were ready for the new Regulation.

### 7.2.5 Improving HR policies

#### The Welcome Kit

To improve the welcome experience for new staff members, the HRBA team put together a *Welcome Kit*. The kit provides newcomers with practical information about working for the EDPS. This includes information on who we are and what we do, time management, learning and development, the medical service and security matters, among many other things.

We hope that by providing new staff members with all this information as part of one kit, we will help them to settle more quickly and easily into working life at the EDPS.

#### Mentorship Programme

The EDPS Mentorship Programme is aimed at all new staff members. Its objective is to facilitate the integration of newcomers into our institution. The rather unique nature of the EDPS as the EU's smallest institution makes the Mentorship Programme useful even for those new staff members who join us from other EU institutions.

Though the Mentorship Programme has been in place since the EDPS itself was established, we found that many staff members were unaware of what being a mentor involves. To address this problem, we developed some guidelines for EDPS staff members, explaining the programme and the role of a mentor in more detail.

A mentor is able to provide support and guidance for a new member of staff, reducing the stress associated with starting a new job. It is also a relationship which can and should be consolidated over the course of the mentee's employment at the EDPS. There are benefits for both sides. The mentee is able to turn to the mentor for help in resolving problems, integrating within the organisation, asserting their professional identity and learning new skills. The mentor benefits from the satisfaction of helping others and the opportunity to view the organisation from a different perspective, and might even learn new ways of approaching issues and tasks from the mentee.

### Active seniors

The *Active Senior* initiative seeks to capitalise on the expertise of retired colleagues to ensure that their skills and knowledge are not lost. This is a new practice for the EDPS, launched on 29 May 2018.

The process is voluntary, both for the retired staff member and the EDPS unit or sector involved. While benefitting from the expertise of a former official may bring added value to our work, we also recognise that it must not replace the work of a current EDPS employee.

Through drawing on their voluntary assistance, we aim to put the expertise of those who have now retired from their work at the European institutions to good use, whatever their seniority level when they retired.

### Making sure good work is always recognised

Our most recent EDPS staff survey showed that a good number of EDPS staff members feel motivated and willing to go the extra mile in their jobs. However, there is always room for improvement.

In 2018 we launched some guidelines aimed at helping managers and other relevant staff members to give better recognition for the work done by their teams. The guidelines explain how to identify what types of recognition are appreciated by different people and the best ways of providing this recognition.

There is no magic formula that works for everyone, so it is important that managers think carefully about this subject, to ensure that their teams receive adequate recognition for their work. This will help to increase motivation among staff members and ensure that they keep doing a great job.

### The Business Continuity Plan

The Internal Audit Service (IAS) requested a thorough revision and update of our Business Continuity Plan

(BCP). We completed this process in 2018 and the BCP is now available on the EDPS intranet.

Revision of the Plan involved reformulating a number of the articles in the original BCP. We also needed to complete the Plan's annexes and carry out a Business Continuity management testing exercise, which we did on 14 November 2018. The report on the exercise was sent to the IAS, in compliance with their recommendations.

To follow up on the exercise, the BCP Desk Officer will present an action plan, with the intention of launching an awareness initiative that will help to create and consolidate a business continuity management culture among EDPS staff. It will also be used to carry out other useful testing exercises.

### Learning and Development

The current EDPS Learning and Development (L&D) strategy was developed in 2015 and is put into practice every year. 2018 was no exception.

EDPS staff members were asked to reflect on the outcomes of their annual appraisal interviews with their respective line manager and produce a personal Learning and Development Plan for 2018-2019.

In addition to the catalogue of courses provided by the European Commission, we set up some in-house training sessions, including:

- Lunchtime sessions on tools and procedures used at the EDPS and the EDPB, aimed at new staff members;
- Training courses to prepare staff for the new Regulation for EU institutions and for the GDPR;
- Management team training on sharing and implementing a vision for the future while building engaged teams;
- Staff training sessions to raise awareness of unconscious biases, to help prevent burnout and stress and on finding the right balance between our professional and private lives.

We also organised a number of communication training courses throughout the year. These were aimed at supporting certain staff members and the Supervisors in their preparations for the [2018 International Conference of Data Protection and Privacy Commissioners](#) (see [section 4.7](#)).

## 8. The Data Protection Officer at the EDPS

### 8.1 THE DPO AT THE EDPS

With the [General Data Protection Regulation](#) (GDPR) now a reality, we face the task of living up to the high expectations of EU citizens and others. Not only do they expect their personal data to be better protected, they expect regulators to keep their promises and demonstrate that they are up to the challenge of enforcing these new rules.

Yet even this is not enough. Regulators must lead by example. When they process personal data, entrusted to them by individuals, they must ensure that they uphold the highest of standards in ensuring the protection of individuals.

The compliance of EU institutions with data protection law was under public scrutiny even before the new rules outlined in [Regulation 2018/1725](#), applicable to their activities, came into force on 11 December 2018 (see [section 4.1.2](#)). The EU cannot credibly call for organisations and businesses operating in the EU to comply with EU rules if its own institutions do not demonstrate that they, too, are compliant. Similarly, as the EU's [data protection authority](#), the EDPS cannot expect to be trusted and taken seriously as a supervisory authority if we are not able to demonstrate our own compliance.



With this in mind, the DPO office at the EDPS, with the support of the whole institution, set up a project to manage our transition process and ensure compliance with the new rules set out under [Regulation 2018/1725](#). The protection of personal data can no longer be treated as a simple exercise in compliance. It requires a

continuous effort from the whole institution, geared towards ensuring the accountable use of personal information, whether we are auditing EU institutions, managing complaints, responding to enquiries, or carrying out any other tasks required of us under EU law.

### 8.2 THE TRANSITION TO A NEW REGULATION

The transition project implemented at the EDPS included:

- examining our data processing activities and identifying the risks they pose to individuals' fundamental rights and freedoms;
- preparing personal data records based on Article 31 of the new Regulation, as well as new data protection notices, which are required for increased transparency;
- reviewing the way in which we manage enquiries from individuals who wish to exercise their data protection rights;
- creating an internal procedure to manage possible breaches of the personal data we process;
- drafting new DPO implementing rules and the necessary internal rules on restrictions to personal data rights based on Article 25 of the new Regulation;
- examining all activities in which we act as joint controllers, relevant written agreements, our relationships with our processors and relevant contracts.

By 11 December 2018, when the new Regulation came into force, we had put in place all of the necessary groundwork for compliance. We will complete the remaining steps in the transition project in 2019.

Our efforts will not end here, however. We plan to set up a framework within the EDPS, supported by top management, that will enable us to provide what we have termed *protection by design*. This will mean fully integrating data protection accountability into the culture of our institution, providing the highest level of protection for the data entrusted to us. This is not an easy task, but we believe that we are more than up to the challenge.

### 8.3 ADVISING THE INSTITUTION AND IMPROVING THE LEVEL OF PROTECTION

Of course, our activities have not only focused on preparing for the future. Throughout the majority of the year, the EU institutions remained bound by the rules outlined in the previous Regulation, [Regulation 45/2001](#).

As in the past, the EDPS DPO office provided advice on a number of processing operations and internal policies based on the rules set out in Regulation 45/2001. We dedicated particular attention to EDPS websites, focusing on the use of cookies for aggregated statistics, as well as on the finalisation of the new website and app for the [2018 International Conference of Data Protection and Privacy Commissioners](#). We also improved the way in which the collection and processing of personal data is carried out when organising meetings and events.

### 8.4 ENQUIRIES AND COMPLAINTS

In 2018, we received 11 enquiries, of which nine concerned requests for access to an individual's own personal data, processed by the EDPS, and two concerned requests for the erasure of personal data.

We also received two complaints. One concerned an event participant's alleged unlawful use of contact details shared, based on consent, by other participants. We ensured that the situation was resolved and the data erased. Another complaint alleged a subcontractor's unlawful use of personal data belonging to an event participant. We supported the complainant, in a situation where the subcontractor had used the data on their own initiative and not on instructions from the EDPS.

We are now receiving an increasing number of enquiries and complaints. This trend is likely to continue now that individuals have more and stronger rights under the new data protection rules and are also more aware of these rights.

### 8.5 AWARENESS-RAISING WITHIN THE EDPS

The EDPS DPO welcomed many new staff members and trainees in 2018. Each new arrival at the EDPS

meets the DPO for a short personal data protection induction meeting, targeted to the educational and professional background of each new staff member and their future role at the EDPS. Some of the topics covered include:

- an introduction to basic data protection concepts and the applicable legal basis;
- the role of the DPO at the EDPS and in the EU institutions;
- preparations for the new data protection rules;
- how the DPO can help staff to exercise their data protection rights.

Internal EDPS coordination and information meetings and the DPO sections on the EDPS intranet and website are also opportunities to reach out to EDPS staff members and external stakeholders and keep them up to date with our activities.

### 8.6 COLLABORATION WITH DPOS IN THE OTHER EU INSTITUTIONS

The biennial meetings of the DPOs of the EU institutions, bodies and agencies are a valuable opportunity for the EDPS DPO to discuss common issues and share experiences and best practices with other DPOs ([see section 4.3.1](#)).

This year, the EDPS organised the DPO network meeting which took place on 30 May 2018, in cooperation with the DPO of the European Parliament. The event, which proved to be the last meeting before the adoption of the new rules, was a great success. 120 DPOs and assistant DPOs took part, contributing to the presentation of case studies and discussions on the main issues encountered as part of their preparations for the new Regulation.

The EDPS DPO Office also participated in the first DPO network meeting of the new era, which took place on 11 December 2018, the day on which the new Regulation entered into force. All DPOs left the meeting with a heightened sense of responsibility, aware of the role we must play in championing personal data protection as project managers for accountability in the EU institutions.

# Annex A - Legal framework

The European Data Protection Supervisor was established by [Regulation \(EC\) No 45/2001](#) of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The Regulation was based on Article 286 of the EC Treaty, now replaced by Article 16 of the [Treaty on the Functioning of the European Union](#) (TFEU). The Regulation also laid down appropriate rules for the institutions and bodies in line with the then existing EU legislation on data protection. It entered into force in 2001. A revised version of the Regulation, [Regulation \(EU\) No 2018/1725](#), entered into force on 11 December 2018.

Since the entry into force of the Lisbon Treaty on 1 December 2009, Article 16 TFEU must be considered as the legal basis for the EDPS. Article 16 underlines the importance of the protection of personal data in a more general way. Both Article 16 TFEU and Article 8 of the [EU Charter of Fundamental Rights](#) establish that compliance with data protection rules should be subject to control by an independent authority. At the 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 ([see section 4.1.3](#)).

## 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 (EC) No 45/2001

Taking a closer look at Regulation 45/2001, it should be noted first that, according to Article 3(1), it applies to the *processing of personal data by Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which are within the scope of Community law*. However, since the entry into force of the Lisbon Treaty and the abolition of the pillar structure – as a result of which references to *Community institutions* and *Community law* have become outdated – the Regulation in principle covers all EU institutions and bodies, except to the extent that other EU acts specify otherwise.

The definitions and the substance of the Regulation closely follow the approach of Directive 95/46/EC. It could be said that Regulation (EC) No 45/2001 is the implementation of this Directive at EU institution level. This means that the Regulation deals with general principles like fair and lawful processing, proportionality and compatible use, special categories of sensitive data, information to be given to the data subject, rights of the data subject, obligations of controllers — addressing special circumstances at EU level where appropriate — and with supervision, enforcement and remedies. A separate chapter deals with the protection of personal data and privacy in the context of internal telecommunication networks. This chapter is the implementation at EU institution level of the former Directive 97/66/EC on privacy and communications.

## Regulation (EC) 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 will only apply 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 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 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 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 to develop further (see section 4.4.1).

## Tasks and powers of the EDPS

The tasks and powers of the EDPS are clearly described in Chapter V, in particular in Articles 41, 46 and 47 of Regulation 45/2001. This is replaced by Chapter VI and Articles 52, 57 and 58 of Regulation 2018/1725 (see Annex B), both in general and in specific terms. Article 41 of Regulation 45/2001 (Article 52 of Regulation 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 and specified in

Articles 46 and 47 of Regulation 45/2001 and Articles 57 and 58 of Regulation 2018/1725 with a detailed list of tasks and powers.

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 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 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 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 2018/1725 now allows for the implementation of one single model for coordinated supervision of **large scale information systems** and of Union bodies, offices or agencies by the EDPS and national supervisory authorities.

# Annex B - Extract from Regulation (EU) 2018/1725

## Article 41 — Information and consultation

1. The Union institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures and internal rules relating to the processing of personal data by a Union institution or body, whether alone or jointly with others.
2. The Union institutions and bodies shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in Article 25.

## Article 42 — Legislative consultation

1. The Commission shall, following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the European Data Protection Supervisor where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.
2. Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may also consult the European Data Protection Board. In such cases the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issuing a joint opinion.
3. The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or if otherwise appropriate, the Commission may shorten the deadline.
4. This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.

## Article 52 — European Data Protection Supervisor

1. The European Data Protection Supervisor is hereby established.
2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies.
3. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and of any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends, the European Data Protection Supervisor shall fulfil the tasks set out in Article 57 and exercise the powers granted in Article 58.
4. Regulation (EC) No 1049/2001 shall apply to documents held by the European Data Protection Supervisor. The European Data Protection Supervisor shall adopt detailed rules for applying Regulation (EC) No 1049/2001 with regard to those documents.

## Article 57 — Tasks

1. Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:
  - a) monitor and enforce the application of this Regulation by Union institutions and bodies, with the exception of the processing of personal data by the Court of Justice acting in its judicial capacity;

- b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
  - c) promote the awareness of controllers and processors of their obligations under this Regulation;
  - d) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the national supervisory authorities to that end;
  - e) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
  - f) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
  - g) advise, on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;
  - h) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
  - i) adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 48(2);
  - j) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39(4);
  - k) participate in the activities of the European Data Protection Board;
  - l) provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;
  - m) give advice on the processing referred to in Article 40(2);
  - n) authorise contractual clauses and provisions referred to in Article 48(3);
  - o) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2);
  - p) fulfil any other tasks related to the protection of personal data; and
  - q) establish his or her Rules of Procedure.
2. The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.
  3. The performance of the tasks of the European Data Protection Supervisor shall be free of charge for the data subject.
  4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

## Article 58 — Powers

1. The European Data Protection Supervisor shall have the following investigative powers:
  - a) to order the controller and the processor to provide any information it requires for the performance of his or her tasks;
  - b) to carry out investigations in the form of data protection audits;
  - c) to notify the controller or the processor of an alleged infringement of this Regulation;
  - d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of his or her tasks;
  - e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law.

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;
  - f) to order the controller to communicate a personal data breach to the data subject;
  - g) to impose a temporary or definitive limitation including a ban on processing;
  - h) 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;
  - i) 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;
  - j) 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.

## Annex C – List of Data Protection Officers

Council of the European Union (CONSILIUM)	<i>Reyes OTERO ZAPATA</i>
European Parliament (EP)	<i>Secondo SABBIONI</i>
European Commission (EC)	<i>Martin KRÖGER</i>
Court of Justice of the European Union (CURIA)	<i>Sabine HACKSPIEL</i>
Court of Auditors (ECA)	<i>Johan VAN DAMME</i>
European Economic and Social Committee (EESC)	<i>Constantin CHIRA-PASCANUT</i>
Committee of the Regions (CoR)	<i>Michele ANTONINI</i>
European Investment Bank (EIB)	<i>Pelopidas DONOS</i>
European External Action Service (EEAS)	<i>Emese SAVOIA-KELETI</i>
European Ombudsman (EO)	<i>Juliano FRANCO</i>
European Data Protection Supervisor (EDPS)	<i>Massimo ATTORESI</i>
European Data Protection Board (EDPB)	<i>Joao SILVA</i>
European Central Bank (ECB)	<i>Barbara EGGL</i>
European Anti-Fraud Office (OLAF)	<i>Veselina TZANKOVA</i>
Translation Centre for the Bodies of the European Union (CdT)	<i>Martin GARNIER</i>
European Union Intellectual Property Office (EUIPO)	<i>Mariya KOLEVA</i>
Agency for Fundamental Rights (FRA)	<i>Nikolaos FIKATAS</i>
Agency for the Cooperation of Energy Regulators (ACER)	<i>Marina ZUBAC</i>
European Medicines Agency (EMA)	<i>Stefano MARINO</i>
Community Plant Variety Office (CPVO)	<i>Mariya KOLEVA</i>
European Training Foundation (ETF)	<i>Tiziana CICCARONE</i>
European Asylum Support Office (EASO)	<i>Alexandru GEORGE GRIGORE</i>
European Network and Information Security Agency (ENISA)	<i>Athena BOURKA</i>
European Foundation for the Improvement of Living and Working Conditions (EUROFOUND)	<i>Maria-Angeliki STAMATOPOULOU</i>
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	<i>Ignacio VÁZQUEZ MOLINÍ</i>
European Food Safety Authority (EFSA)	<i>Claus REUNIS</i>
European Maritime Safety Agency (EMSA)	<i>Radostina NEDEVA</i>
European Centre for the Development of Vocational Training (CEDEFOP)	<i>Robert STOWELL</i>
Education, Audiovisual and Culture Executive Agency (EACEA)	<i>Panagiota KALYVA</i>
European Agency for Safety and Health at Work (EU-OSHA)	<i>Michaela SEIFERT</i>
European Fisheries Control Agency (EFCA)	<i>Marta RAMILA HIDALGO</i>
European Union Satellite Centre (EUSC)	<i>Esther MOLINERO</i>
European Institute for Gender Equality (EIGE)	<i>Ramunas LUNSKUS</i>
European GNSS Agency (GSA)	<i>Ezio VILLA</i>

European Railway Agency (ERA)	Zografia PYLORIDOU
Consumers, Health and Food Executive Agency (CHAFAEA)	Tobias KOHLHOF
European Centre for Disease Prevention and Control (ECDC)	Andrea IBER
European Environment Agency (EEA)	Olivier CORNU
European Investment Fund (EIF)	Paolo SINIBALDI
European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)	Nayra PEREZ
European Securities and Markets Authority (ESMA)	Sophie VUARLOT-DIGNAC
European Aviation Safety Agency (EASA)	Stephan MICK
Executive Agency for Small and Medium-sized Enterprises (EASME)	Elke RIVIERE
Innovation and Networks Executive Agency (INEA)	Caroline MAION
European Banking Authority (EBA)	Joseph MIFSUD
European Chemicals Agency (ECHA)	Bo BALDUYCK
European Research Council Executive Agency (ERCEA)	Cristina GANGUZZA
Research Executive Agency (REA)	Evangelos TSAVALOPOULOS
European Systemic Risk Board (ESRB)	Barbara EGGL
Fusion for Energy (ITER)	Angela BARDENHEWER-RATING
SESAR Joint Undertaking (SESAR)	Laura GOMEZ GUTIERREZ
Electronic Components and Systems for European Leadership (ECSEL)	Anne SALAÛN
Clean Sky Joint Undertaking (CLEAN SKY JOINT)	Bruno MASTANTUONO
Innovative Medicines Initiative Joint Undertaking (IMI JU)	Sebastien PECHBERTY
Fuel Cells & Hydrogen Joint Undertaking (FCH)	Georgiana BUZNOSU
European Insurance and Occupations Pensions Authority (EIOPA)	Catherine COUCKE
European Police College (CEPOL)	Ioanna PLIOTA
European Institute of Innovation and Technology (EIT)	Nora TOSICS
European Defence Agency (EDA)	Clarisse RIBEIRO
Body of European Regulators for Electronic Communications (BEREC)	Geoffrey DEVIN
European Union Institute for Security Studies (EUISS)	Nikolaos CHATZIMICHALAKIS
European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)	Fernando Luis POCAS DA SILVA
Shift2Rail Joint Undertaking (S2R JU)	Isaac GONZALEZ GARCIA
Single Resolution Board (SRB)	Esther BRISBOIS
Europol (EUROPOL)	Daniel DREWER
Bio-Based Industries joint Undertaking (BBI JU)	Marta CAMPOS ITURRALDE

# Annex D - List of prior check and non-prior check opinions

## Administration

### Anti-fraud, whistleblowing and finance

- Administrative Inquiries and Disciplinary Proceedings, (EBA), 25 July 2018 (2017-1083)
- Administrative inquiries, (EIB), 18 July 2018 (2017-1071)
- Conduct of investigations by the Security Office of the General Secretariat of the Council (GSC), (COUNCIL), 25 April 2018 [UPDATE] (2017-0216)
- Whistleblowing, (EMSA), 3 April 2018 (2017-0303)
- Whistleblowing, (EMCDDA), 22 March 2018 (2016-1083)
- Whistleblowing, (FRA), 21 March 2018 (2016-0737)
- Whistleblowing and relevant internal fraud issues, (REA), 21 March 2018 (2014-0178)
- Whistleblowing, (EDPS), 15 March 2018 (2017-0493)
- Whistleblowing, (ECHA), 15 March 2018 (2015-1029)
- Administrative inquiries and disciplinary proceedings, (EIT), 17 January 2018 (2016-1165)

### Administration and Human Resources

- Security Investigations, (EEAS), 7 December 2018 (2017-1107)
- ILOAT and EFTA Court complaints in the field of HR, (EFTA), 23 November 2018 (2017-1141)
- Security verifications on employees of external contractors requiring access to EUIs, (EEAS), 30 October 2018 (2016-0894)
- Security Verification of External Resources, (EUIPO), 15 October 2018 (2017-0350)
- Accreditation and Notification of Diplomats by Union Delegations to the Host Country, (EEAS), 5 October 2018 (2017-1099)

- Reasonable accommodation, (COUNCIL), 18 September 2018 (2018-0592)
- Disciplinary and Grievance Investigations, (EFTA), 18 September 2018 (2017-1142)
- Selection of Confidential Counsellors, (EIF), 18 September 2018 (2017-1043)
- Informal procedure for cases of harassment, (EIF), 18 September 2018 (2017-1042)
- Security Clearances, (ESA), 18 September 2018 (2017-1004)
- Occupational activity after leaving service, (EO), 19 July 2018 (2017-1064)
- Underperformance management, (EC), 19 July 2018 (2017-0395)
- Staff Reclassification, (EACEA), 10 July 2018 (2017-1062)
- Health data, (GSA), 10 July 2018 (2018-0589)
- CSISLA - Reimbursement Request for Medical Expenses, (EEAS), 3 July 2018 (2017-0986)
- Performance Management, (EFTA), 20 June 2018 (2017-1094)
- Health data, (EIOPA), 24 May 2018 (2017-0284)
- Access and use of the Ombudsman's e-mail system, (EO), 12 April 2018 (2017-1059)
- Harassment, (EIOPA), 10 April 2018 (2017-0916)
- Repatriation of EU expatriate staff on medical grounds, (EEAS), 4 April 2018 (2016-0778)
- Meetings Organisation, (ECDG), 20 March 2018 (2017-1078) - Non Prior Check
- OHC Pregnancy Self-Assessment Data, (EIB), 12 March 2018 (2016-0614)

- Management of all leave entitlements processing of received requests for reimbursement of annual medical check-ups received pre-employment medical exams/clearances, (SRB), 8 March 2018 (2017-0853)
- Mobility procedure, (COUNCIL), 21 February 2018 (2018-0031)
- Social and financial aid social assistance and advice on reimbursement of medical expenses for Headquarters and EU Delegations, (EEAS), 21 February 2018 (2016-0779)
- Administrative and financial data related to the individual rights of staff members, (SRB), 9 February 2018 (2017-0852) - Non Prior Check
- Time management module of Sysper, (SRB), 7 February 2018 (2017-0850) - Non Prior Check
- First-aid intervention registers, (COUNCIL), 26 January 2018 (2017-0969)
- Access to ECDC premises, (ECDC), 17 January 2018 (2017-1077) - Non Prior Check
- Grants, (EIT), 10 December 2018 (2017-1070)
- Grants Management, (CHAFEA), 10 December 2018 (2017-1068)
- H2020 Grants Award and Management (INEA), 10 December 2018 (2017-1037)
- Grant management in Participant portal, (EASME), 10 December 2018 (2017-0977)
- Registration Selection and Management of Independent Experts in the context of the FP7 and Horizon 2020 (H2020) Framework Programmes, (REA), 25 September 2018 (2017-1085)
- Independent expert management Horizon 2020, (SESAR JU), 25 September 2018 (2017-1075)
- Experts H2020, (BBI), 25 September 2018 (2017-1073)
- Management of experts, (EACEA), 25 September 2018 (2017-1063)
- Independent Expert Management, (CHAFEA), 25 September 2018 (2017-1053)

### Evaluation (360° and Staff Appraisal)

- Probationary Period Reports, (GSA), 9 October 2018 (2017-1066)
- Promotion and reclassification, (CDT), 26 September 2018 (2016-0292)
- Staff appraisal, (CDT), 26 September 2018 [UPDATE] (2016-0011)
- Promotion, (EUSC), 6 September 2018 (2014-0603)
- Staff Appraisal, (EACEA), 10 July 2018 (2017-1061)
- Multi-source feedback reviews for managers, (COUNCIL), 18 Apr 2018 (2018-0170)
- Statistics on individual production and timeliness, (EUIPO), 8 March 2018 (2017-0841)
- Selection and management of Independent Experts for the implementation of parts of H2020, (INEA), 25 September 2018 (2017-1038)
- Experts management in Participant portal, (EASME), 25 September 2018 (2017-0976)
- Experts management outside Participant portal, (EASME), 31 July 2018 (2017-1040)
- Grants management outside Participant portal, (EASME), 31 July 2018 (2017-1039)
- Experts management outside Participant portal COSME programme, (EASME), 31 July 2018 (2017-1036)
- Grant management outside Participant portal COSME programme, (EASME) 31 July 2018 (2017-1035)

### Grants and Public Procurement

- Grants Award and Management in the context of Horizon 2020 Framework Programme, (REA), 10 December 2018 (2017-1080)
- Management and award of grants Horizon 2020, (SESAR JU), 10 December 2018 (2017-1076)
- Contract Renewal Process, (EBA), 19 July 2018 (2017-1082)
- Contractual renewal, (EIOPA), 31 May 2018 (2017-0769)
- Procurement procedures, (EASME), 22 March 2018 (2017-1058)

- Independent Experts Management, (FCH 2JU), 30 January 2018 (2018-0030)
- Grant award and management, (FCH 2JU), 30 January 2018 (2018-0029)

### Recruitment

- Selection recruitment and administrative management of Local Agents (LA) in EU Delegations, (EEAS), 30 November 2018 (2017-1106)
- Selection Recruitment and Administrative Management for international staff in CSDP Missions by the EEAS Civilian Planning and Conduct Capability (CPCC), (EEAS), 6 November 2018 (2017-1105)
- Selection procedure for ECDC, (EC), 16 October 2018 (2018-0039)
- Recruitment, (EIB), 6 September 2018 [UPDATE] (2015-1052)
- Recruitment, (EIB), 6 September 2018 (2017-1072)
- Recruitment, (EFTA), 20 June 2018 (2017-1093)
- Recruitment Temporary staff, (EMSA), 6 June 2018 (2015-0439)
- Selection Recruitment and Administrative Management for Junior Professionals in EU Delegations (JPDs), (EEAS), 13 March 2018 (2016-0772)
- Recruitment of Staff: TAs SNEs and trainees, (SRB), 2 March 2018 (2017-0851)
- New starters and leavers, (EFTA), 22 February 2018 (2017-1143) - Non Prior Check
- Selection and administrative management of Blue book trainees in EEAS Headquarters and in EU Delegations, (EEAS), 12 February 2018 (2016-0771)

- Selection and recruitment of TA CA SNE trainees and interims, (S2R JU), 8 February 2018 (2018-0119)
- Recruitment procedure Executive Director, (CEPOL), 29 January 2018 (2017-0787)

### Core Business

- Automated security analysis of SSL-encrypted internet services used from the EEAS network, (EEAS), 7 December 2018 (2015-0593) - Non Prior Check
- DG SANTE's new notification 'AAC system', (EC), 29 October 2018 (2017-0803)
- Application for Return (FAR), (FRONTEX), 26 September 2018 (2017-0874)
- Updating the current Mutual Assistance Broker (MAB), (EC), 24 September 2018 (2018-0698)
- International Child Abduction Mediator Activity, (EP), 12 September 2018 (2016-0731)
- Social media monitoring, (ECB), 21 March 2018 (2017-1052)
- Erasmus+ Online Linguistic Support scheme, (EACEA), 1 March 2018 (2014-1154) - Non Prior Check
- Erasmus+ Online Linguistic Support scheme, (EACEA), 1 March 2018 (2014-1154) - Non Prior Check
- Stakeholder Quality Assurance Panel (SQAP), (EUIPO), 20 February 2018 (2017-0845)
- EU autonomous restrictive measures, (COUNCIL), 5 February 2018, [update to 2012-0725], (2018-0106)

# Annex E – List of Opinions and formal comments on legislative proposals

## Opinions

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

In 2018 the EDPS issued Opinions on the following subjects (date of publication in brackets):

- Commission Package on free and fair European elections ([18 December 2018](#))
- Upgrading the Visa Information System ([13 December 2018](#))
- A New Deal for Consumers ([5 October 2018](#))
- Security of identity cards and residence documents of EU citizens and their family members ([10 August 2018](#))
- Digital tools and processes in company law ([26 July 2018](#))
- Public Sector Information (PSI) re-use Directive ([10 July 18](#))
- Privacy by Design ([31 May 2018](#))
- Interoperability between EU large-scale information systems ([16 April 2018](#))
- Online manipulation and personal data ([19 March 2018](#))
- Exchange of data between Europol and third countries ([14 March 2018](#))
- Proposal for Council Regulation on jurisdiction decisions in matrimonial matters and the matters of parental responsibility and on international child abduction (Brussels II recast) ([15 February 2018](#))

## Formal Comments

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

In 2018 the EDPS issued formal comments on the following subjects (date of publication in brackets):

- European Border and Coast Guard ([3 December 2018](#))
- Covered bonds and covered bonds public supervision ([12 October 2018](#))
- Facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences ([10 September 2018](#))
- Insurance against civil liability in respect of the use of motor vehicles ([26 July 2018](#))
- Review of OLAF Regulation ([24 July 2018](#))
- Migration and international protection ([18 July 2018](#))
- Fisheries controls ([18 July 2018](#))
- Copyright in the Digital Single Market ([3 July 2018](#))
- Free-flow of non-personal data in the European Union ([8 June 2018](#))
- European Labour Authority (ELA) ([30 May 2018](#))
- Screening of foreign direct investments into the European Union ([12 April 2018](#))
- VAT fraud and administrative cooperation ([8 March 2018](#))
- Visa Information System (VIS) to include data on long stay visas and residence documents ([9 February 2018](#))

# Annex F – Speeches by the Supervisor and Assistant Supervisor in 2018

## European Parliament

Assistant Supervisor, *Data protection and privacy aspects of the current generation of Event Data Recorders and advanced drowsiness monitoring*, speech during the hearing on *Type-approval Requirements for Motor Vehicles as regards their general Safety and the Protection of Vehicle Occupants and Vulnerable Road Users*, European Parliament, Brussels (29 November 2018).

Assistant Supervisor, speech at LIBE hearing on e-Evidence, European Parliament, Brussels (27 November 2018).

Assistant Supervisor, speech at the third meeting of the Joint Parliamentary Scrutiny Group on Europol, European Parliament, Brussels (25 September 2018).

Supervisor, speech at the LIBE hearing on the Facebook/Cambridge Analytica case, European Parliament, Brussels (25 June 2018).

Assistant Supervisor, *Data Protection Issues in Artificial Intelligence & High Performing Computing*, speech at the seminar *Data Driven Innovation & AI Conference Data*, European Parliament, Brussels (6 June 2018).

Assistant Supervisor, speech at *No Interruptions: options for the future UK-EU data sharing arrangement*, European Parliament, Brussels (5 June 2018).

Supervisor, speech at the Fifth World Congress for Freedom of Scientific research, European Parliament, Brussels (12 April 2018).

Supervisor, speech to LIBE on Annual Report 2017, European Parliament, Brussels (20 March 2017).

Supervisor, *EDPS supervision of Europol: 2017 activities and ongoing work*, speech at the meeting of the Joint Parliamentary Scrutiny Group on Europol, European Parliament, Brussels (19 March 2018).

Assistant Supervisor, speech at the second meeting of the Joint Parliamentary Scrutiny Group on Europol, Sofia, Bulgaria (19 March 2018).

Assistant Supervisor, speech at *Information session on the Reform of the Data Protection Regulation*, Data Protection Day, European Parliament, Luxembourg (31 January 2018).

## Council

Assistant Supervisor, DAPIX meeting on interoperability, Brussels (18 April 2018).

Assistant Supervisor, *Quantum of personal information stored in PNR drops down to national info-reservoirs*, speech at the conference *The practical implementation of the Passenger Name Record Directive*, Sofia, Bulgaria (21 February 2018).

Assistant Supervisor, *GDPR from a Political and Regulatory Point of View*, speech at the conference *General Data Protection Regulation*, Sofia, Bulgaria (29 January 2018).

## European Commission

Assistant Supervisor, *Free and fair elections and an informed and pluralistic democratic debate. Practical steps to ensure that the online world supports an informed and pluralistic democratic debate*, speech at the Annual Colloquium on Fundamental Rights 2018 “Democracy in the EU”, Brussels (26-27 November 2018).

Assistant Supervisor, *Digitalisation of the energy sector - challenges and benefits for consumers. Privacy issues and solutions*, speech during The EU Sustainable Energy Week - EUSEW 2018 - conference, Brussels (5-6 June 2018).

## Other EU institutions and bodies

Assistant Supervisor, *Moving away from freedom v. security tune*, speech at the Academy of European Law (ERA) conference on Freedom and Security, The Hague, The Netherlands (22-23 November).

Assistant Supervisor, *Future perspectives of privacy engineering*, speech at the Annual Privacy Forum 2018, Barcelona, Spain (13-14 June 2018).

Assistant Supervisor, video speech at AGH University, Krakow, Poland (6 June 2018).

Assistant Supervisor, *Radar Watchkeeping: Have you monitored your Communication department's radar to avoid collisions with the new Regulation?* speech at EDPS-DPO meeting, Brussels (31 May 2018).

## International conferences

Assistant Supervisor, *Facilitating Data Transfers*, contribution to the seminar *Regulating Personal Data in an Innovation Economy: UK-French Perspectives*, Paris, France (6 December 2018).

Assistant Supervisor, *Global Development of Privacy Law and Brexit: The difference between deal and no-deal*, speeches at Data Protection World Forum, Privacy, trust, risk, security, London, United Kingdom (20-21 November 2018).

Supervisor, video contribution to the Data Protection Africa Summit, Mauritius (19-23 November 2018).

Assistant Supervisor, *Right to Privacy in Digital Era*, speech at the conference *Flourishing in a data-enabled society*, Buckinghamshire, United Kingdom, (1 November 2018).

Supervisor, closing speech at *Debating Ethics: Dignity and Respect in a Data Driven Life*, 40th International Conference of Data Protection and Privacy Commissioners, European Parliament, Brussels (25 October 2018).

Assistant Supervisor, *Move Slower and Fix Things*. Report from the Creative Room, speech at the 40th International Conference of Data Protection and Privacy Commissioners, Brussels (21-25 October 2018).

Assistant Supervisor, *Basic features of data protection in the humanitarian context*, speech at the workshop *2nd Working Series of Data Protection Guidelines for Humanitarian Actions*, side event at the 40th International Conference of Data Protection and Privacy Commissioners, Brussels (21-25 October 2018).

Assistant Supervisor, speech at the workshop *Convention 108+: the Global Data Protection Convention*, side event at the 40th International Conference of Data Protection and Privacy Commissioners, Brussels (21-25 October 2018).

Assistant Supervisor, speech at the workshop *The future for collective action under the GDPR (Art. 80)*,

side event at the 40th International Conference of Data Protection and Privacy Commissioners, Brussels (21-25 October 2018).

Assistant Supervisor, *Artificial Intelligence in humanitarian actions*, speech at the workshop *From Privacy to Ethics: Misuse, Missed Use, and the Public Good*, side event at the 40th International Conference of Data Protection and Privacy Commissioners, Brussels (21-25 October 2018).

Supervisor, *Choose Humanity: Putting Dignity back into Digital*, opening speech at 40th International Conference of Data Protection and Privacy Commissioners, Brussels (24 October 2018).

Assistant Supervisor, *New technology, data collection and privacy – where can we find the balance?* speech at the 6th Annual Conference QED nt. "Cybersecurity, Brussels (17 October 2018).

Assistant Supervisor, *ICT's next wave – balancing connectivity and privacy*, speech at the FT-ETNO Summit 2018 pt. Review, Reboot, Revive: a Future Agenda for Europe, Brussels (15 October 2018).

Assistant Supervisor, *Surveillance for Public Security Purposes. Four pillars of acceptable interference in fundamental right to privacy*, speech at the conference *Right to privacy in the digital age*, Warsaw, Poland (20-22 September 2018).

Assistant Supervisor, *General Data Protection Regulation (GDPR) as a Key to Better Control in the Processing of Personal Data*, speech at the seminar *Aplicació del Reglament europeu de protecció de dades, primers passos*, Barcelona, Spain (14 June 2018).

Assistant Supervisor, *Privacy by Design in Theory and in Real World*, speech at the 7th Internet Privacy Engineering Network (IPEN) workshop organised by the EDPS and the Universitat Politècnica de Catalunya, Barcelona, Spain (13 June 2018).

Assistant Supervisor, *The Notion of 'Personal Data' in Utilities Sectors*, video contribution to the conference *GDPR: A Positive Change for Utility Companies?* Sofia, Bulgaria (13 June 2018).

Assistant Supervisor, *Leveraging Transnational Networks* speech at the conference *Agora Forum: Steady As She Goes? The EU Navigating Today's Complex World*, Brussels (7-8 June 2018).

Assistant Supervisor, *Many Paths of the Reform of Data Protection Law in Europe* speech at the conference

*Personal Data Protection in Poland and Belgium*, Brussels (5 June 2018).

Supervisor, Austrian Commission of Jurists, Vienna, Austria (31 May 2018).

Supervisor, video contribution to the 8th European Data Protection Days (EDPD), Berlin, Germany (14 May 2018).

Assistant Supervisor, speech at the *Global state of data protection roundtable* at RightsCon 2018, Toronto, Canada (16-18 May 2018).

Supervisor, 4th International Congress 2018 ASSO DPO, Milan, Italy (8 May 2018).

Assistant Supervisor, *The protection of personal data in the framework of police and judicial institutions*, speech at the Spring Conference, Tirana, Albania (3-4 May 2018).

Assistant Supervisor, *Social media, micro-targeting and political campaigning: challenges and opportunities for data protection authorities*, speech at the Spring Conference, Tirana, Albania (3-4 May 2018).

Assistant Supervisor, *Automated Individual Decision-Making and Profiling under the GDPR – How the GDPR addresses the concepts?* speech at the Annual Conference on European Data Protection Law 2018 Focus on the General Data Protection Regulation, Brussels (19-20 April 2018).

Assistant Supervisor, *Importance of GDPR*, speech at *GDPR and Marketing*, GSMA Mobile World Congress, GSMA Ministerial Programme, Barcelona, Spain (26-28 February 2018).

Supervisor, video contribution to The Moroccan international conference on privacy and data protection in Africa- CNDP, Casablanca, Morocco (22 February 2018).

Supervisor, video contribution to the Commonwealth Data Forum 2018, Gibraltar (21-23 February 2018).

Supervisor, Closing remarks by Giovanni Buttarelli given at the 11th International Computers, Privacy and Data Protection Conference, Brussels (25 January 2018).

Assistant Supervisor, *Regulating for Results*, speech at Computers, Privacy and Data Protection (CPDP) 2018, *Internet of Bodies*, Brussels (24-26 January 2018).

## Other events

Supervisor, video contribution to Il regolamento europeo sulla privacy (gdpr): alcune riflessioni sugli impatti, Rome, Italy (20 December 2018).

Supervisor, video contribution to Giornata della Trasparenza, Prevenzione della corruzione, trasparenza e privacy: quale bilanciamento?, Venice, Italy (20 December 2018).

Supervisor, video contribution to Advanced Competition Seminar, European University Institute (EUI), Florence, Italy (15 December 2018).

Supervisor, video contribution to Annual Human Rights Conference, Tallin, Estonia (10 December 2018).

Supervisor, video contribution to 2018-2019: Data Protection: un biennio rivoluzionario, Roma-Camera dei Deputati, Rome, Italy (11 December 2018).

Supervisor, video contribution to Conference on Artificial Intelligence, Warsaw, Poland (30 November 2018).

Assistant Supervisor, *Sześć miesięcy stosowania RODO. Europejska perspektywa na pierwsze doświadczenia*, speech at the conference Konwentu Ochrony Danych i Informacji 2018, Łódź, Poland (23 November 2018).

Supervisor, *Convegno nazionale Siamo tutti spiati? per la 17a edizione del premio P.Piazzano di giornalismo scientifico*, Novara, Italy (17 November 2018).

Assistant Supervisor, *Modern threats (terrorism & cyber security) and access to electronic data: data protection regulations & other limitations in the area of justice and security*, speech at The Security Trade Council of European Confederation of Independent Trade Unions, Brussels (15 November 2018).

Supervisor, video contribution to AGI Presidenza: Invito ad intervenire al Convegno nazionale AGI, Bologna, Italy (27 October 2018).

Supervisor, video contribution to Life after the GDPR: good data protection rules and prospects for the future, Szeged, Hungary (22-26 October 2018).

Supervisor, video contribution to Cosa Sarà, la trasformazione digitale è la nostra vita quotidiana Pavia, Italy (19-21 October 2018).

Supervisor, video contribution to DECODE Symposium 2018, Beyond surveillance capitalism: in search of Europe's digital sovereignty, Barcelona, Spain (16-17 October 2018).

Assistant Supervisor, Accountability Tools for Public Institution. Experiences of EU institutions, agencies and bodies, speech at the workshop Accountability under the GDPR – How to Implement, Demonstrate and Incentivise it, Paris, France (5 October 2018).

Supervisor, video contribution to CHAM2018, Building the European Health System, Paris, France (28-29 September 2018).

Supervisor, video contribution to Friends of Europe - European Young Leaders' seminar, Valletta, Malta (13-15 September 2018).

Supervisor, video contribution to Industrial Revolution 4.0: Digital Economics, Data Protection & Compliance Best-Practice, Latvia (7-8 September 2018).

Supervisor, video contribution to UnionCamere - La disciplina europea in materia di tutela della privacy ed il registro delle imprese, Rome, Italy (9 July 2018).

Supervisor, Life after the GDPR: good data protection rules and prospects for the future, Brussels (27 June 2018).

Supervisor, speech at the Ambassadorial Cocktail Reception for ICDPPC 2018, Brussels (5 June 2018).

Assistant Supervisor, Problemy Społeczne i Zawodowe Informatyki, speech at the University of Warsaw, Warsaw, Poland (29 May 2018).

Assistant Supervisor, Zakres terytorialny obowiązywania RODO a najbliżsi sąsiedzi Unii Europejskiej, speech at the 10th conference Security in Internet pt. Ochrona danych osobowych, Warsaw, Poland (25 May 2018).

Assistant Supervisor, Ogólne rozporządzenie o ochronie danych jako część reformy bezpieczeństwa danych w Europie. Czym jest RODO w świecie NIS / eIDAS / ePrivacy / AML / PSD2 / eEvidence/ eFracht etc., speech at the scientific conference Wyzwania prawne związane z początkiem stosowania Ogólnego Rozporządzenia o Ochronie Danych (RODO), Gdansk, Poland (28 April 2018).

Supervisor, Privacy, data protection and cyber security in the era of AI, Brussels (24 April 2018).

Assistant Supervisor, The Impact of the General Data Protection Regulation on Financial Institutions, speech

at the 9th FinanzplatzFrühstück (Financial Centre Breakfast), Frankfurt, Germany (17 April 2018).

Assistant Supervisor, introductory speech at the conference High-Level Working Roundtable on Tax and Revenue Collection in the Era of Data Protection: How Agencies Can Make Challenge an Opportunity, Brussels (16 April 2018).

Assistant Supervisor, Essential guarantees of data protection in law enforcement sector in the era of interoperable large scale IT systems, lecture during the celebration of the 15th anniversary of European Digital Rights (EDRi), Brussels (12 April 2018).

Assistant Supervisor, Czy nowy ład prawny zadziała w praktyce? Rola organów ochrony danych, sądów i TSUE w wykładni prawa ochrony danych osobowych, speech at the conference 4. Forum Prawa Mediów Elektronicznych, GDPR, Wrocław, Poland (10-11 April 2018).

Assistant Supervisor, Dokumentacja przetwarzania danych osobowych w instytucjach Unii Europejskiej, speech at the technological conference Nowe zasady zabezpieczania danych osobowych, czyli RODO w praktyce, Warsaw, Poland (28 March 2018).

Supervisor, speech at Diritto ed economia delle piattaforme digitali, Roma TRE University, Rome, Italy (22 March 2018).

Supervisor, video contribution to Auditel Conference at the Italian Chamber of Deputies, Rome, Italy (15 February 2018).

Supervisor, video contribution to Le regole sono cambiate: privacy UE 679/16, Pordenone, Italy (23 February 2018).

Supervisor, video contribution to Auditel Conference at the Italian Chamber of Deputies, Rome, Italy (15 February 2018).

Assistant Supervisor, Création du CEPD et les dernières guidelines, speech at the 14e Conférence Annuelle Nouveau reglement data protection, Paris, France (8 February 2018).

Supervisor, video contribution to the Westminster eForum Keynote Seminar: Data protection and the developing regulatory framework, Brussels (25 January 2018).

Supervisor, video contribution to La rivoluzione Europea della Privacy, Regulation EU 679/2016, Padova, Italy (22 January 2018).

# Annex G - Composition of EDPS Secretariat



## Director and Private Office

Leonardo CERVERA NAVAS  
*Director*

Christian D'CUNHA  
*Head of Private Office of the EDPS*

Ernani CERASARO  
*Policy Administrative Assistant*

Anna COLAPS  
*Policy Assistant*

Sylvie PICARD  
*Internal Control Coordinator*

Maria José SALAS MORENO  
*Administrative Assistant*

Martine VERMAUT  
*Administrative Assistant*

## Supervision and Enforcement

Delphine HAROU  
*Ad interim Head of Unit*

Petra CANDELIER  
*Head of Complaints and Litigation*

Bénédicte RAEVENS  
*Head of EUROPOL Supervision*

Ute KALLENBERGER  
*Head of Inspections*

Owe LANGFELDT  
*Head of Consultations*

Stephen ANDREWS  
*Supervision and Enforcement Assistant*

Guillaume BYK  
*Legal Officer*

Evanthia CHATZILIASI  
*Legal Officer*

Graça COSTA  
*Legal Officer*

Fanny COUDERT  
*Legal Officer*

Elena FIERRO  
*Legal Officer*

Barbara GIOVANELLI  
*Digital Ethics Policy Officer*

Dirk HOMANN  
*Legal Officer*

Xanthi KAPSOSIDERI  
*Legal Officer*

Anna LARSSON STATTIN  
*Legal Officer/Seconded National Expert*

Francoise MAYEUR  
*Supervision and Enforcement Assistant*

Anne NOEL  
*Supervision and Enforcement Assistant*

Maria Veronica PEREZ ASINARI  
*Legal Officer*

Aikaterini POULIOU  
*Legal Officer*

Snezana SRDIC  
*Legal Officer*

Tereza STRUNCOVA  
*Legal Officer*

Zsofia SZILVASSY  
*Legal Officer*

## Policy and Consultation

Anna BUCHTA  
*Ad interim Head of Unit*

Olivier MATTER  
*Head of International cooperation*

Zsuzsanna BELENYESSY \*  
*Legal Officer*

Sandra BETTI  
*Policy and Consultation Assistant*

Veronique CIMINA  
*Legal Officer*

Priscilla DE LOCHT  
*Legal Officer*

Claire GAYREL  
*Legal Officer*

Mario GUGLIELMETTI  
*Legal Officer*

Amanda JOYCE  
*Policy and Consultation Assistant*

Laurent LIM  
*Legal Officer*

Sophie LOUVEAUX  
*Legal Officer*

Claire-Agnes MARNIER  
*Legal Officer*

Lara SMIT  
*Legal Officer*

Matthias WILDPANNER-GUGATSCHKA  
*Legal Officer/Seconded National Expert*

Agnieszka ZAPOROWICZ  
*Legal Officer*

## IT Policy

Achim KLABUNDE  
*Head of Sector*

Massimo ATTORESI  
*Technology and Security Officer*  
*Data Protection Officer*

Andy GOLDSTEIN  
*Technology and Security Officer*  
*LISO*

Dina KAMPOURAKI  
*Technology and Security Officer*

Malgorzata LAKSANDER \*  
*Technology and Security Officer*

Xabier LAREO  
*Technology and Security Officer*

Frederik LINDHOLM  
*Administrative Assistant*

Robert RIEMANN  
*Technology and Security Officer*

## Records Management

Luisa PALLA  
*Head of Sector*

Marta CÓRDOBA HERNÁNDEZ  
*Administrative Assistant*

Kim Thien LÊ  
*Administrative Assistant*

Séverine NUYTEN  
*Administrative Assistant*

Constantin STANCU  
*Archivist*

Maria TIGANITAKI  
*Administrative Assistant*

## Information and Communication

Olivier ROSSIGNOL  
*Head of Sector*

Francesco ALBINATI  
*Information and Communication Officer*

Isabelle BARON  
*Information and Communication Officer*

Thomas HUBERT  
*Graphic Designer Assistant*

Courtenay MITCHELL  
*Information and Communication Officer*

Veronica MORO  
*Information and Communication Officer*

Parminder MUDHAR  
*Information and Communication Officer*

Agnieszka NYKA  
*Information and Communication Officer*

Benoit PIRONET  
*Web Developer*

Filippo SEGATO  
*Information and Communication Officer*

## Human Resources, Budget and Administration

Marian SANCHEZ LOPEZ  
*Ad interim Head of Unit*

Cláudia BEATO  
*HR Assistant*

Pascale BEECKMANS  
*HR Assistant*  
GEMI

Laetitia BOUAZZA-ALVAREZ  
*HR Assistant*  
GECO  
LSO  
*Traineeship Coordinator*

Angelo FASSARI  
*Administrative Assistant*

Sebastian GALEA  
*Finance Assistant*

Laurent HAMERS  
*Finance Assistant*

Sophie JEANNON  
*Administrative Assistant*

Julia MOLERO MALDONADO  
*Finance Assistant*

Marco MORESCHINI  
*HR Officer/Seconded National Expert*  
LSO

Carolina POZO-LOPEZ\*  
*Finance Assistant*

Karina REMPESZ  
*HR Officer*  
*L&D Coordinator*

Anne-Françoise REYNDERS  
*HR Officer*

Jean- Michel VERSTAEN  
*Finance Assistant*

Christophe WALRAVENS  
*Procurement and Finance Officer*

Caroline WOUSSEN-DUBUISSEZ\*  
*Finance Assistant*

## **EDPB Secretariat**

Isabelle VEREECKEN  
*Head of the EDPB Secretariat*

Katinka BOJNAR  
*Legal Officer/Seconded National Expert*

Hannelore DEKEYSER  
*Legal Officer*

Greet GYSEN  
*Information and Communications Officer*

Sarah HANSELAER  
*Information and Communications Officer*

Ahmed IMMOUN  
*Technology and Security Officer*

Joelle JOURET  
*Legal Officer*

Zoi KARDASIADOU  
*Legal Officer/Seconded National Expert*

Peter KRAUS  
*Technology and Security Officer*

Fabienne MOLLET  
*Administrative Assistant*

Hanna OBERSTELLER  
*Legal Officer/Seconded National Expert*

Effrosyni PANAGOY  
*Assistant of the EDPB Secretariat*

Andrei PETROVICI  
*Technology and Security Assistant*

Romain ROBERT  
*Legal Officer*

Luis SEGURA  
*Archivist*

João SILVA  
*Legal Officer*  
*DPO*

Jasminka TOKALIC  
*Administrative Assistant*

Anne- Marie VANDENBERGHEN  
*Administrative Assistant*

Anna ZAWILA-NIEDZWIECKA  
*Legal Officer/Seconded National Expert*

\*staff members who left the EDPS in the course of 2018







## 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.

