

EUROPEAN DATA PROTECTION SUPERVISOR



ANNUAL | 2016  
REPORT

An Executive Summary of this report which gives an overview of key developments in EDPS activities in 2016 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.

**Europe Direct is a service to help you find answers  
to your questions about the European Union.**

**Freephone number (\*):  
00 800 6 7 8 9 10 11**

(\* ) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the Internet (<http://europa.eu>).

Luxembourg: Publications Office of the European Union, 2017

Print	ISBN 978-92-9242-111-3	ISSN 1830-5474	doi:10.2804/807674	QT-AA-17-001-EN-C
PDF	ISBN 978-92-9242-110-6	ISSN 1830-9585	doi:10.2804/250895	QT-AA-17-001-EN-N
EPUB	ISBN 978-92-9242-109-0	ISSN 1830-9585	doi:10.2804/36979	QT-AA-17-001-EN-E

© European Union, 2017

© Photos: iStockphoto/EDPS & European Union

Reproduction is authorised provided the source is acknowledged.

*Printed in Luxembourg*

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)



ANNUAL  
REPORT | 2016

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>
1.1 <b>Supervision and Enforcement</b>	<b>9</b>
1.2 <b>Policy and Consultation</b>	<b>9</b>
1.3 <b>Monitoring technology</b>	<b>10</b>
<b>2. 2016 - An Overview</b>	<b>11</b>
2.1 <b>Preparing for the changes to come</b>	<b>11</b>
2.2 <b>Moving the global debate forward</b>	<b>11</b>
2.3 <b>EU institutions leading by example</b>	<b>11</b>
2.4 <b>A responsible approach to EU policy</b>	<b>12</b>
2.5 <b>Internal administration</b>	<b>13</b>
2.6 <b>Communicating our message</b>	<b>13</b>
2.7 <b>Key Performance Indicators 2016</b>	<b>13</b>
<b>3. Main Objectives for 2017</b>	<b>15</b>
<b>4. 2016 Highlights</b>	<b>18</b>
4.1 <b>Responding to new challenges</b>	<b>18</b>
4.1.1 Legislative reform	18
4.1.2 Advising the EU institutions	19
4.1.3 EDPS initiatives	21
4.2 <b>EU borders and security</b>	<b>21</b>
4.2.1 Securing Europe's rights and borders	21
4.2.2 Catching up with criminal records	22
4.2.3 Smart Borders need smart policies	22
4.2.4 A Common European Asylum System that respects fundamental rights	23
4.2.5 Bordering on privacy: EDPS continues work with Frontex	23
4.2.6 Effective supervision of large-scale IT systems	23
4.2.7 Coordinated supervision of large-scale IT systems	24
4.2.8 Observing Schengen	24
4.2.9 Security vs. Privacy: the encryption debate continues	24
4.3 <b>On the ground</b>	<b>25</b>
4.3.1 The EDPS guide to securing information	25

4.3.2	Protecting privacy in online communication	25
4.3.3	Guidelines for going mobile	26
4.3.4	Whistleblowing in the EU institutions	26
4.3.5	Dealing with rule-breakers in the EU institutions	26
4.3.6	The DPO function: EU institutions leading by example	27
4.3.7	A privacy-friendly cloud?	27
4.3.8	A Reference Library for data protection	28
4.3.9	Protecting privacy in the EU institutions	28
4.3.10	Transparency vs. protection of personal data	30
4.3.11	Data protection for social workers	33
4.3.12	A healthy approach to data protection	33
4.3.13	Partners in compliance	36
4.3.14	Catching up with the institutions: inspections and visits	36
<b>4.4</b>	<b>International cooperation</b>	<b>36</b>
4.4.1	International data transfers	36
4.4.2	International cooperation	37
<b>4.5</b>	<b>Beyond compliance</b>	<b>40</b>
4.5.1	The Accountability Initiative	40
4.5.2	An ethical approach to fundamental rights	41
4.5.3	Putting the GDPR into practice	42
4.5.4	Keeping track of new technology	42
4.5.5	Practical preparations for the EDPB	43
4.5.6	Europol: a new supervisory role for the EDPS	44
<b>5</b>	<b>Court Cases</b>	<b>45</b>
5.1	EU-Canada PNR faces scrutiny	45
<b>6</b>	<b>Transparency and Access to Documents</b>	<b>46</b>
<b>7</b>	<b>The Secretariat</b>	<b>47</b>
<b>7.1</b>	<b>Information and communication</b>	<b>47</b>
7.1.1	Online media	47
7.1.2	Events and publications	48
7.1.3	External relations	49
7.1.4	Preparations for the EDPB	49
<b>7.2</b>	<b>Administration, budget and staff</b>	<b>51</b>
7.2.1	Budget and finance	51
7.2.2	Human Resources	52
<b>8</b>	<b>The Data Protection Officer at the EDPS</b>	<b>54</b>
<b>8.1</b>	<b>The DPO at the EDPS</b>	<b>54</b>
<b>8.2</b>	<b>Leading by example</b>	<b>54</b>
<b>8.3</b>	<b>Advising the institution and improving the level of protection</b>	<b>54</b>
<b>8.4</b>	<b>The register of processing operations</b>	<b>54</b>
<b>8.5</b>	<b>Providing information and raising awareness</b>	<b>54</b>

Annex A - Legal framework	55
Annex B - Extract from Regulation (EC) No 45/2001	57
Annex C - List of Data Protection Officers	59
Annex D - List of prior check and non-prior check opinions	61
Annex E - List of Opinions and formal comments on legislative proposals	64
Annex F - Speeches by the Supervisor and Assistant Supervisor in 2016	65
Annex G - Composition of EDPS Secretariat	69

## TABLES AND GRAPHS

Figure 1. EDPS KPI analysis table	14
Figure 2. Evolution of the number of complaints received by EDPS	31
Figure 3. EU institutions and bodies concerned by complaints received by EDPS	31
Figure 4. Type of violation alleged in complaints received by EDPS	32
Figure 5. Evolution of Notifications received by EDPS	34
Figure 6. Evolution of prior check Opinions issued by EDPS	35
Figure 7. Percentage split between Core Business and Administration activities in the Notifications received by EDPS	35



## | Foreword

Many momentous events took place in 2016, the longer-term implications of which it is too early to predict. The EU, however, has almost certainly done the work of a generation with its regulatory reforms for data protection. The General Data Protection Regulation (GDPR) and the Directive for data protection in the police and justice sectors, which entered the statute book last year, may turn out to be a major step forward not only for fundamental rights in the digital age but also, as the positive outcome of years of tortuous negotiations, for European democracy.

The GDPR has been, and will continue to be, the point of reference for our work. As set out in the Strategy for our mandate, we aim to make data protection as simple and effective as possible for all involved. The GDPR is of strategic importance for our institution because it lays out the parameters for data processing and supervision in the EU institutions themselves. We have been actively promoting the concept of accountability to leaders of EU institutions and bodies, offering them practical tools to help them ensure and demonstrate compliance. Through our work as an enforcer and ombudsman for individual concerns, we have experienced first-hand the increasing public awareness of the importance of protecting personal data. People are more conscious than ever of what can happen if their personal information is not handled responsibly; it is our duty, and that of all data protection authorities (DPAs), to ensure that it is.

Like other DPAs, and as enforcers and advisors to those responsible for proposing, scrutinising and reviewing legislation, we have invested considerable energy in preparing for the new rules. We are working in close collaboration with the Article 29 Working Party, to ensure that we are able to provide an effective and efficient secretariat to the new European Data Protection Board, and have deepened and intensified our loyal cooperation with other regulatory authorities around the world.

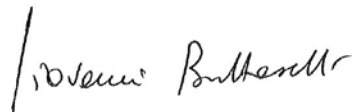
We also recognise that if DPAs are to be effective, they must be fully conversant with data driven technologies. Our background paper on Artificial Intelligence represents one exercise in that direction. As technology continues to develop, DPAs will need to make sure that we are prepared for the changes it will bring.

Data flows are a global reality and 2016 marked a potential turning point in how they are regulated. We advised the EU legislator on the Umbrella agreement and the Privacy Shield, concerning the transfer of data from the EU to the United States, and engaged with data protection and privacy commissioners from every continent, to help build a new consensus on rights in the digital era.

We recognise that data protection law does not operate in a vacuum, and in January 2016 we launched the Ethics Advisory Group. This group of six eminent individuals, each an expert in their own distinct field, is charged with developing innovative and effective ways of ensuring EU values are upheld in an era of ubiquitous data and intelligent machines. We also set up a Digital Clearing House for competition, consumer and data authorities to share information and ideas on how to ensure the individual interest is best served in specific cases.

One of the innovations of the GDPR is the requirement for each controller to appoint a data protection officer (DPO). The EU institutions, thanks to Regulation 45/2001, have almost two decades of experience working with DPOs. We hope and believe that, with our support, EU institutions will become a beacon for responsible data processing; an example which controllers in the private and public sectors can aspire to.

Our priority will be to make this happen.



**Giovanni Buttarelli**  
European Data Protection Supervisor



**Wojciech Wiewiórowski**  
Assistant Supervisor



# Mission statement, values and principles

Everyone in the European Union is entitled to the protection of their personal data. 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. Established under [Regulation \(EC\) No. 45/2001](#), 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 the Regulation, the EU as a policymaking, legislating and judicial entity looks to the EDPS as an independent supervisor for impartial advice on policies and proposed laws which might affect the rights to privacy and data protection. The EDPS performs this function through developing itself as a centre of excellence in the law, but also in technology insofar as it affects or is affected by the processing of personal information.

We carry out our functions in close cooperation with fellow data protection authorities in the [Article 29 Working Party](#), and aim to be as transparent as possible in our work serving the EU public interest.

We are guided by the following values and principles in our approach to our tasks and how we work with our stakeholders:

## 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 policy and 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 impact on privacy. We act selectively and proportionately.

# | EDPS Strategy 2015-2019

The [EDPS Strategy 2015-2019](#) was adopted on 2 March 2015. 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 European Data Protection Supervisor (EDPS) finalised a strategy for the coming five years. His aim was to turn his vision of an EU that leads by example in the debate on data protection and privacy into reality and to identify innovative solutions quickly.

This 2015-2019 Plan summarises:

- the major data protection and privacy challenges over the coming years;
- 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 lessons learned from implementing our [Strategy 2013-2014: Towards Excellence in Data Protection](#).

## Vision, Objectives and Action 2015-2019

The EDPS' 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 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 is responsible for ensuring that the European institutions and bodies respect fundamental rights when processing personal data and developing new policies. We have three main fields of work:

- **Supervision:** Monitoring the processing of personal data in the EU administration and ensuring compliance with [data protection rules](#). Our tasks range from prior checking processing operations likely to present specific risks, to handling complaints and conducting inquiries.
- **Consultation:** Advising the European Commission, the European Parliament and the Council on proposals for new legislation and on other issues which impact data protection.
- **Cooperation:** Working with national [data protection authorities](#) (DPAs) to promote consistent data protection throughout Europe. Our main platform for cooperation with DPAs is the [Article 29 Working Party](#) (WP29).

The data protection rules with which the EU institutions must comply, and which the EDPS is required to enforce, are set out in [Regulation 45/2001](#). All other organisations which operate in the EU must comply with the [Data Protection Directive](#), which is enforced at national level by each of the national DPAs.

However, new EU data protection rules, designed for the digital age, will apply from 25 May 2018. The Data Protection Directive will be replaced by the [General Data Protection Regulation](#) (GDPR), finalised at the end of 2015, whilst Regulation 45/2001, which outlines the roles and responsibilities of the EDPS, will be revised in 2017, to bring it in line with the GDPR.

Our work is therefore focused not only on ensuring compliance with current legislation but anticipating and preparing for the changes to come, as is reflected in our [Strategy 2015-2019](#).

## 1.1 SUPERVISION AND ENFORCEMENT

Our supervision and enforcement work aims to promote a culture of data protection in the EU institutions and bodies. We ensure that they are not only aware of their obligations, but can also be held accountable for

complying with them. There are several ways in which we do this:

- **Carrying out prior checks:** All EU institutions and bodies are required to inform the EDPS of any planned procedures which might pose a risk to the protection of personal data. We examine the proposals and provide recommendations on how to address these risks.
- **Dealing with complaints:** We handle complaints from individuals relating to the processing of personal data in the EU institutions. The EDPS investigates these complaints and decides on the best way to handle them.
- **Monitoring compliance:** The EDPS is responsible for ensuring that all EU institutions and bodies comply with Regulation 45/2001. We monitor compliance in various ways, including visits, [inspections](#), and our biennial general survey of the EU institutions.
- **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.
- **Providing guidance:** The EDPS issues [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 must appoint a [DPO](#), who is responsible for ensuring that the institution complies with data protection rules. We work closely with DPOs, providing them with training and support to ensure that they are able to perform their role effectively.

## 1.2 POLICY AND CONSULTATION

The EDPS acts as an advisor on data protection issues in a wide range of policy areas. Our policy and consultation work aims to ensure that data protection requirements are integrated into all new legislation. We do this by providing guidance on proposed legislation to both the European Commission, as the policy initiator,

and the European Parliament and the Council, as co-legislators. We use several tools to help us:

- **EDPS Priorities:** Each year, we publish a list of priorities, based on the Commission's work plan. We focus our efforts on areas which present the highest risk for non-compliance or where the impact on privacy and data protection is greatest. We also use the work programme of the [WP29](#) as an important point of reference.
- **Informal Comments:** In line with established practice, the EDPS is consulted informally by the Commission 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.
- **Formal Opinions:** These relate to proposals for legislation and are addressed to all three EU institutions involved in the legislative process. We use them to highlight our main data protection concerns and our recommendations. Opinions are available to read on our website as well as in the Official Journal of the EU.
- **Formal Comments:** Like our Opinions, our formal Comments address the data protection implications of legislative proposals. However, they are usually issued in response to Commission communications, which set out an area of future enquiry for EU policy. We publish them on our website.
- **Court Cases:** We can intervene and offer our data protection expertise before the EU courts either at the Court's invitation or on behalf of one of the parties in a case.
- **Cooperation with national DPAs:** We cooperate with national DPAs through the [WP29](#), which provides the European Commission with independent advice on data protection issues and contributes to the development of harmonised data protection policies across the EU. 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 TECHNOLOGY

Technology is advancing at a considerable pace and many new technologies rely on personal data to perform their function. It is therefore important that data protection and privacy measures adequately address these new developments.

The EDPS IT Policy team is charged with monitoring technological developments and their impact on data protection and privacy. Knowledge and expertise in this area is necessary in order to effectively perform our supervision and consultation tasks. Our activities include:

- **Monitoring and responding to technological developments:** We monitor technological developments, events and incidents and assess their impact on data protection in order 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 develop engineering practices which incorporate privacy concerns and to encourage engineers to build privacy mechanisms into internet services, standards and apps.
- **Keeping track of IT at the EDPS:** In our role as Supervisor to the EU institutions, we believe we should set the standard for data protection compliance. We are therefore continually monitoring and improving the technology used by the EDPS to ensure that it works effectively and efficiently whilst remaining in line with data protection requirements.

## | 2. 2016 - An Overview

In our [Strategy 2015-2019](#), we outlined our vision of an EU which leads by example in the global dialogue on data protection and privacy in the digital age. On 4 May 2016 the [GDPR](#) was published in the Official Journal of the European Union, marking a big step towards achieving this goal. The GDPR will help shape a global, digital standard for privacy and data protection, centred on individuals, their rights and freedoms and their personal identity and security. However, much work still remains if we are to ensure that our vision becomes a reality.

### 2.1 PREPARING FOR THE CHANGES TO COME

Much of our work in 2016 focused on preparing for and implementing the GDPR. We worked in close cooperation with our colleagues in the [WP29](#) to help draft guidance on the new legislation, but also to ensure that we are prepared for the responsibility of both providing the secretariat and acting as an independent member of the new European Data Protection Board (EDPB).

Under the new legislation, the EDPB will replace the WP29, taking on responsibility for ensuring that the GDPR is applied consistently across the EU. It is therefore vital that the EDPB be fully operational by 25 May 2018, when the GDPR becomes applicable and enforceable. Throughout 2016, we worked with the WP29 to start developing rules of procedure, and to analyse options for IT, budget and service level agreements for the new body.

If Europe is to remain at the forefront of the debate on data protection and privacy we also need a modern legal framework for ePrivacy, which both guarantees the fundamental right to the confidentiality of communications and complements the protections offered by the GDPR. At the Commission's request, we issued a preliminary [Opinion](#) on the proposal for a revised ePrivacy Directive in July 2016. We will continue to advocate for a smarter, clearer and stronger Directive, the scope of which adequately reflects the technological and societal realities of the digital world, throughout the negotiation process.

### 2.2 MOVING THE GLOBAL DEBATE FORWARD

As part of our Strategy, we committed to developing an ethical dimension to data protection. In January 2016

we set up the [Ethics Advisory Group](#) to examine digital ethics from a variety of academic and practical perspectives. Our aim was to initiate an international debate on the ethical dimension of data protection in the digital era.

The group held their first workshop in May 2016. They will continue their work through to 2018, when they will present their findings at the International Conference of Data Protection and Privacy Commissioners, which will be hosted by the EDPS and the Bulgarian DPA.

The closed session of the 2016 International Conference focused on an equally forward-looking subject: the implications of Artificial Intelligence, machine learning and robotics for data protection and privacy. The EDPS Strategy outlines our dedication to ensuring that data protection goes digital. We therefore sought to inform and steer the debate on this topic through issuing a very well-received [background document](#) for discussion at the conference.

Technology continues to develop at a rapid pace and it is essential that all data protection authorities, including the EDPS, make sure that they are ready for the challenges this will bring. To help address these challenges, the EDPS launched [IPEN](#) in 2014. Composed of IT experts from all sectors, the group provides a platform for cooperation and information exchange on engineering methods and tools which integrate data protection and privacy requirements into new technologies. The adoption of the GDPR, which requires anyone responsible for processing personal data to observe the principles of [data protection by design](#) and by default, has heightened the profile of the group and its work and encouraged researchers, developers and data protection regulators to increase their efforts to strengthen and improve the technological dimension of data protection.

### 2.3 EU INSTITUTIONS LEADING BY EXAMPLE

However, achieving our goal of establishing the EU as a leader in data protection on the global stage depends first on the EU institutions setting the standard at European level. As the independent authority responsible for supervising the processing of personal data at this level, we have been working with the EU institutions and bodies to help them prepare for the changes to come. Though the GDPR does not apply to

their activities, the rules that do will be updated during the course of 2017, to bring them in line with the GDPR.

In 2016, we continued our efforts to develop and deepen our cooperation with the [DPOs](#) of the EU institutions and bodies. As those responsible for ensuring that their respective institutions comply with data protection law, DPOs are our closest partners at the institutional level. Throughout the year we have worked with them on both a collective and individual level to prepare them for the changing rules. This included introducing them to new concepts, such as [Data Protection Impact Assessments](#), which are likely to become mandatory under the new rules, as they are under the GDPR, as well as continuing to provide guidance in the form of [Guidelines](#) and [prior-check Opinions](#). We also sought their input on the revision of [Regulation 45/2001](#) before providing advice on this to the legislator.

The GDPR includes an explicit reference to the principle of [accountability](#), which it is safe to assume will also be applied to the EU institutions and bodies. It requires that technical and organisational measures be put in place by organisations, transferring the responsibility for demonstrating compliance away from [DPAs](#) and DPOs, and to the organisations themselves. In 2016, we launched the EDPS Accountability Initiative, designed to equip EU institutions, beginning with the EDPS as a data controller itself, to lead by example in how they comply and demonstrate compliance with [data protection rules](#). As part of the initiative, we developed a tool for evaluating accountability, which we tested first on ourselves, as an institution. We then visited and met with the most senior representatives of seven EU bodies to promote the initiative and will continue this process in 2017.

During the course of the year we also issued several [Guidelines](#) for the EU institutions. EDPS Guidelines provide practical advice on how to comply with data protection rules in specific situations. They serve as a reference document against which the institutions can measure their activities and, as such, serve as a valuable tool in improving accountability. Many of our Guidelines are also relevant and applicable to the work of other organisations.

In recognition of the increasingly important role played by digital communication in the everyday work of the EU institutions, we issued Guidelines on [web services](#) and [mobile applications](#) in November 2016. The Guidelines offer practical advice on how to integrate data protection principles into the development and management of web-based services and mobile apps respectively, and incorporate input from relevant experts at the EU institutions and bodies, as well as DPOs, ensuring that they remain relevant in practice

and not just in theory. We also issued a [Guidance document](#) on Information Security Risk Management (ISRM), designed to help those responsible for information security to effectively analyse the data protection risks and determine a set of security measures to be implemented, ensuring both compliance and accountability.

Several of our Guidelines are aimed at helping the EU institutions ensure that they are able to comply with the specifications of the [EU Staff Regulations](#) whilst respecting the rights to privacy and data protection. In July 2016 we published [Guidelines](#) on the processing of personal information as part of a whistleblowing procedure. We provided recommendations on how to create safe channels for staff to report fraud, ensure the confidentiality of information received and protect the identities of anyone connected to the case.

In November 2016 we published [Guidelines](#) on the processing of personal information in administrative inquiries and disciplinary proceedings. These Guidelines provide EU institutions with the legal framework required to carry out administrative inquiries and guarantee that the relevant procedures are implemented in a way that ensures the processing of personal data is lawful, fair, transparent and complies with their data protection obligations.

The EDPS has also been preparing to take on a new supervisory responsibility. Under the new legal framework for Europol, approved on 11 May 2016, the EDPS will take over responsibility for supervising the processing of personal data at Europol, as well as providing the secretariat for a new Cooperation Board. This Board will help facilitate cooperation between ourselves and national DPAs in cases relating to data from the Member States. The new role presents a new challenge which both the EDPS and Europol will endeavour to fulfil in a way which reflects the professionalism and reliability of the EU institutions in the field of data protection.

## 2.4 A RESPONSIBLE APPROACH TO EU POLICY

Upholding the credibility of the GDPR internationally requires ensuring that the high standard it sets is promoted in all EU policy. In our role as an advisor to the Commission, the Parliament and the Council, we aim to ensure that this is the case. Two particularly high-profile areas in which the EU sought to develop new policy in 2016 were international data transfers and border management.

Following the 2015 annulment of the Safe Harbour decision by the EU Court of Justice, the Commission negotiated a new adequacy decision with the United

States, on which we were consulted in 2016. In our [Opinion](#) on the Privacy Shield, which provides for the transfer of data from the EU to the US, we called for a stronger self-certification system, whilst emphasising the need for more robust safeguards on US public authorities' access to personal data, and improved oversight and redress mechanisms.

We also issued an [Opinion](#) on the EU-US umbrella agreement on the protection of personal data transferred between the EU and the US for law enforcement purposes. In our recommendations, we highlighted the need to ensure that the agreement upholds fundamental rights, particularly in relation to the right to judicial redress. We also emphasised the need for improved safeguards for all individuals and stressed the importance of clarifying that, under the agreement, the transfer of sensitive data in bulk is prohibited.

Border policy remained a particularly high priority for the EU in 2017, resulting in several new EU policy initiatives aimed at keeping EU borders safe and secure. Legislation in this area raises particularly difficult questions related to balancing the need for security with the right to data protection.

In 2016 we issued [recommendations](#) on how to ensure that the rights of migrants and refugees are respected, in response to the proposed European Border and Coast Guard Regulation. We followed up on this by providing [advice to Frontex](#) on how to use the powers granted to them under the new Regulation to effectively handle personal data in risk analysis relating to people smuggling.

We also issued Opinions on the Commission's revised proposal to establish an [Entry/Exit System](#) (EES) for all non-EU citizens entering and exiting the EU, and on the [Common European Asylum System](#). In both cases, we asked the Commission to consider if some of the measures proposed were truly necessary to achieve their desired aims.

## 2.5 INTERNAL ADMINISTRATION

To be taken seriously as a supervisory and advisory authority, we must ensure that our own internal administration and data protection practices are adequate and effective. This is even more important considering the administrative function we will provide for the new EDPB.

In 2016, staff from the Human Resources, Budget and Administration (HRBA) Unit at the EDPS worked closely with the EDPS DPO to develop and test our accountability tool. We also implemented internal

policies, such as an ethics framework, aimed at increasing transparency and promoting professionalism.

As part of our preparations for the EDPB, we are responsible for ensuring that the new body receives adequate human and financial resources from the budgetary authority and that the necessary administrative set-up is in place. This work continued to gather pace in 2016, and was documented in a series of EDPB factsheets outlining our vision, aimed at keeping our partners in the WP29 fully informed about our activities.

We also comply fully with our obligation to respond to requests for access to documents and are committed to increasing the transparency of our work, principally through the launch of a new EDPS website in early 2017.

## 2.6 COMMUNICATING OUR MESSAGE

The work we do to establish data protection priorities and take a leading role on the international stage depends on ensuring that our voice is heard.

We communicate our work using a variety of tools, including online media, press, events and publications. Our [app](#) on the GDPR, which was updated in 2016 to include the final adopted versions of the GDPR and the Directive on police, justice and criminal matters, was a particularly successful exercise in transparency and legislative accountability. We also launched a [blog](#) in 2016, aimed at providing a more detailed insight into the work of the Supervisors.

We continue to strive to reach new audiences both online and off, whether through our rapidly growing social media channels or through visits and events.

With the eyes of the world on Europe, the EDPS will continue to work with our data protection partners to make our vision of an EU which leads by example in the global dialogue on data protection and privacy in the digital age a reality.

## 2.7 KEY PERFORMANCE INDICATORS 2016

Following the adoption of the EDPS Strategy 2015-2019 in March 2015, we re-evaluated our key performance indicators (KPIs) to take into account our new objectives and priorities. The new set of KPIs will help us to monitor and adjust, if needed, the impact of our work and our use of resources.

The table below shows our performance in 2016, in accordance with the strategic objectives and action plan defined in the EDPS Strategy.

The KPI scoreboard contains a brief description of each KPI, the results on 31 December 2016 and the set target. The indicators are measured against initial

targets in most cases, but there are two KPIs that have been calculated for the first time: KPI 5 and KPI 9.

The results show that the implementation of the Strategy is on track, with all KPIs meeting or exceeding their respective targets. No corrective measures are therefore needed at this stage.

KEY PERFORMANCE INDICATORS		RESULTS AT 31.12.2016	TARGET 2016
<b>Objective 1 - Data protection goes digital</b>			
KPI 1	Number of initiatives promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	9	9
KPI 2	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8	8
<b>Objective 2 - Forging global partnerships</b>			
KPI 3	Number of initiatives taken regarding international agreements	8	5
KPI 4	Number of cases dealt with at international level (WP29, CoE, OECD, GPEN, International Conferences) for which EDPS has provided a substantial written contribution	18	13
<b>Objective 3 - Opening a new chapter for EU data protection</b>			
KPI 5	Analysis of impact of the input of EDPS on the GDPR and the Directive on police, justice and criminal matters	GDPR: high impact Directive: medium impact	2016 as benchmark
KPI 6	Level of satisfaction of DPOs/DPCs/controllers on cooperation with EDPS and guidance, including satisfaction of data subjects as to training	88%	60%
KPI 7	Rate of implementation of cases in the EDPS priority list (as regularly updated) in form of informal comments and formal opinions	93%	90%
<b>Enablers - Communication and management of resources</b>			
KPI 8	Number of visits to the EDPS website	459 370 visits to the website	2015 as benchmark + 10% (195 715 visits to website; 3631 followers on twitter)
(composite indicator)	Number of followers on the EDPS Twitter account	6122 followers on Twitter	
KPI 9	Level of Staff satisfaction	75%	2016 as benchmark - biennial survey

Figure 1. EDPS KPI analysis table



## | 3. Main Objectives for 2017

The following objectives have been selected for 2017 within the overall Strategy for 2015–2019. The results will be reported in the Annual Report 2017.

### Ensuring confidentiality and privacy in electronic communications

As part of the data protection package which will include the [GDPR](#) and the revision of the rules for EU institutions and bodies, the European Commission also intends to adopt new rules on ePrivacy. We will contribute to the ongoing review of the [ePrivacy Directive](#). Our focus, among other issues, will be on the need to adequately translate the principle of confidentiality of electronic communications, enshrined in Article 7 of the [EU Charter of Fundamental Rights](#) and Article 8 of the [European Convention on Human Rights](#), into EU law.

### Preparing for the revised Regulation 45/2001

In early 2017, the Commission will issue a proposal for a new Regulation to replace the [current rules](#) governing data protection in the EU institutions. The revision of these rules concerns the EDPS directly as it defines our role and powers as a supervisory authority and sets out the rules we will enforce in the EU institutions and bodies. Given its importance, we will devote considerable resources to the revision process in 2017, in order to ensure that the rules for data processing applicable to EU institutions, bodies, offices and agencies are aligned as much as possible with the principles of the GDPR. Once the text is finalised, we will update our internal procedures accordingly and help the EU institutions and bodies to implement the new rules.

### Facilitating the assessment of necessity and proportionality

In 2016 we published a [background paper](#) on necessity (see section 4.1.2) and launched a stakeholder consultation. Taking into account the feedback received, in early 2017 the EDPS will publish a necessity toolkit. It will provide guidance to EU policymakers and legislators responsible for preparing measures which involve the processing of personal

data and which interfere with the right to the protection of personal data. We will follow up with a background document on the principle of proportionality in EU data protection law and will organise workshops devoted to specific EU policy areas, in order to train Commission staff and raise their awareness of data protection issues.

### Promoting stronger borders based on respect for fundamental rights

In an effort to address the migration and internal security challenges faced by the EU, a number of new initiatives have been proposed. The EDPS will continue to offer advice on the data protection implications of EU proposals associated with implementing the Commission's Security Union agenda and Action Plan on terrorist financing. We will also offer advice on several planned initiatives relating to EU borders and security, such as ETIAS, the revision of [SIS II](#) and ECRIS (see section 4.2) and the interoperability of these systems.

We will closely monitor the potential impact on data protection of the new framework for [adequacy decisions](#) on the exchange of personal data with third countries, new trade agreements and possible agreements in the law enforcement sector. In addition, we will continue to consolidate our contacts with the European Parliament and the Council, offering assistance and guidance where necessary.

### Preparing the EU institutions for Data Protection Impact Assessments

A particular focus of our efforts to prepare [DPOs](#) and [controllers](#) in the EU institutions for their new obligations will be on [Data Protection Impact Assessments](#) (DPIAs). DPIAs are part of the broader shift towards [accountability](#), enabling EU institutions to assume responsibility for ensuring compliance. They provide frameworks for assessing the data protection and privacy risks of data processing operations which are considered high risk and help those responsible for processing the data to focus their efforts where they are most needed. We will continue our work on DPIAs in our meetings with the DPO network and will provide individual guidance where needed.

## Guidance on technology and data protection

In 2017 we will issue Guidelines on IT governance and management and on cloud computing. We will also follow up on our Guidelines on [web services](#) and [mobile apps](#) by focusing on their practical implementation in the EU institutions and bodies under our supervision. Based on detailed analysis of specific websites and apps, we will provide practical advice for concrete cases.

## Revising EDPS Guidelines on health data

In 2017 we will revise our existing Guidelines on the processing of data related to health in the workplace and further develop our expertise on big data and health. These Guidelines are needed to account for the significant increase in the processing of data related to health for statistical, research and scientific purposes. Our aim is to highlight all relevant data protection rules and illustrate them with specific examples from our experience dealing with notifications, consultations and complaints. We will actively involve some of the DPOs from the EU institutions and bodies who wish to share their experiences in this area.

## The Spring Survey

Every two years, the EDPS carries out a general survey of EU institutions and bodies. The survey is an effective tool for monitoring and ensuring the application of [data protection rules](#) in the EU institutions, and complements monitoring tools such as visits or inspections. We will carry out our next Survey in 2017.

## Developing our expertise in IT security

We will continue to develop our expertise in IT security and apply them in our inspection and auditing activities. This includes continuing our supervision work on [large-scale information systems](#) and expanding it to new areas, such as the supervision of Europol. We will also use this knowledge as we prepare the infrastructure for the EDPB, in partnership with national [DPAs](#).

## International cooperation

Continued cooperation with national DPAs will be essential in 2017. In addition to continuing our joint preparations for the GDPR, we will work with the [WP29](#) on subjects including the security agenda and new

counter-terrorism measures, international transfers, financial data, health and IT developments. We will also work with DPAs in our role as a European data protection secretariat, not only for the EDPB but also in our work on coordinated supervision of large-scale IT systems and the supervision of Europol.

We will contribute as far as possible to discussions on data protection and privacy in international fora and will continue our dialogue with international organisations, notably through the organisation of a joint workshop in May 2017.

## Accountability project

To account for the impact on EU institutions and bodies of the forthcoming revision of [Regulation 45/2001](#), we will organise information and awareness-raising visits. These visits will focus primarily on encouraging EU institutions to implement the principle of accountability (see section 4.5.1), as well as the specific requirements contained in the new rules on data protection in the EU institutions. With the intention of leading by example, the EDPS Supervision and Enforcement Unit will cooperate with the EDPS DPO to further develop internal implementation of the accountability principle. We will share our experiences with the DPO network.

## Developing an ethical dimension to data protection

Developing an ethical dimension to data protection is one of the [priorities](#) of the current EDPS mandate. The work of the EDPS and the [Ethics Advisory Group](#) (EAG) in 2016 has increased awareness of digital ethics in the data protection community. In 2017, the EDPS will continue to support the work of the EAG and make sure that the worldwide debate on digital ethics remains high on the agenda. The EAG will publish its first Interim Report and organise a workshop alongside the EDPS to reach out to the scientific community. The EDPS will also start integrating ethical insights into our day-to-day work as an independent regulator and policy advisor as well as starting our preparations for the public session of the 2018 International Conference of Data Protection and Privacy Commissioners, which will be hosted by the EDPS and the Bulgarian DPA and will focus on digital ethics.

## Monitoring technology

The EDPS monitors new technologies and assesses their impact on privacy in accordance with our aim to ensure that data protection goes digital, as outlined in

our [Strategy](#). However, our work in this field is not well publicised. We therefore intend to increase the visibility of this work and make our conclusions more accessible through better communication. This might involve the organisation of, or participation in, workshops that will contribute to deepening our analysis and better focus our contributions to public debate. We will continue to develop our cooperation with the EU Agency for Network and Information Security (ENISA) and aim to hold a workshop with academic technology researchers to help improve direct cooperation with academia.

### Data protection goes digital

Article 25 of the GDPR makes [data protection by design](#) and by default a mandatory requirement. This obligation has increased interest in the engineering approach to privacy and inspired new business and research partnerships. [IPEN](#), with its partners in academia, civil society, administration and industry, aims to cooperate with such initiatives. We will continue to improve the network's communication tools and will strengthen cooperation and coherence so as to make launching and supporting new initiatives easier. As the network grows, we will also be able to organise more IPEN events.

### Preparing for the EDPB

The EDPB will replace the WP29 under the GDPR. Since the EDPS will provide the Secretariat for the EDPB, we need to ensure that the EDPB is ready to start work from the day the GDPR becomes fully applicable. The necessary preparatory work will be done in close cooperation with the WP29 and we will ensure that proper transitional arrangements are in place for a smooth handover. We will therefore continue participating in the EDPB-WP29 task force to set up the EDPB secretariat. This work will include ensuring that we have the appropriate IT infrastructure, establishing working methods and rules of procedure and ensuring adequate human and financial resources.

### Effective supervision of Europol

A [new data protection framework](#) for Europol will come into force on 1 May 2017, under which the EDPS will take over responsibility for supervising the processing of personal data at Europol. We have been preparing for this new role at organisational and human resources levels (see section 4.5.6) and will continue to do so until 1 May 2017, when effective supervision will start. Our new role will involve carrying out our standard supervision tasks, including complaint handling, consultations, dealing with requests for information and conducting inspections, as well as cooperating with national supervisory authorities within the newly-established Cooperation Board.

### Setting up the Digital Clearing House

In 2016, we announced our intention to set up a Digital Clearing House (see section 4.1.3). This will bring together agencies from competition, consumer and data protection who are willing to share information and discuss how to enforce rules which support the interests of the individual in the digital space. At the end of 2016, we issued a questionnaire to all agencies willing to participate. In 2017 we will use the results of the questionnaire to discuss practical steps to make the enforcement of rights more effective. We anticipate a meeting of the network in spring 2017, followed by a conference or first public meeting of the Clearing House in autumn 2017.

### Awarding those who apply privacy enhancing technologies

The EDPS wants to encourage designers to implement Privacy Enhancing Technologies (PETs) in new apps. We will therefore create an award for privacy friendly mobile health (mHealth) apps, to be launched in 2017.

## 4. 2016 Highlights

A new EU data protection framework means new challenges for the EDPS. Much of our work in 2016 focused on how to respond to and anticipate the upcoming changes. This included working with the [WP29](#) to prepare for the [GDPR](#) and advising the legislator on the revision of data protection rules for the EU institutions and ePrivacy. We also responded proactively to new legislative proposals and put forward new initiatives, with the intention of consolidating our role as an advisor to the EU institutions on data protection and privacy.

Terrorism and migration continued to rate high on the EU agenda in 2016. The European Commission issued several new proposals designed to keep EU borders secure and the public debate on how to balance the need for security with the right to privacy continued. We monitored and responded to the relevant legislation and followed the relevant debates, whilst also cooperating with national authorities to supervise the processing of personal data in existing [border control systems](#).

One of the main roles of the EDPS is to ensure that EU institutions and bodies comply with [data protection rules](#). Our aim is to ensure that the EU institutions lead by example. We supervised and provided advice to the EU institutions throughout 2016, carrying out inspections, issuing [prior check Opinions](#) and [Guidelines](#) and developing our relationships with the [DPOs](#) responsible for ensuring compliance within their respective EU institutions.

The [EDPS Strategy 2015-2019](#) outlines our aim to develop international partnerships and raise the profile of data protection and privacy globally. In 2016 we contributed fully to European and international fora and actively monitored and provided advice on legal instruments and international agreements with an impact on data protection, including the Privacy Shield and the Umbrella agreement. We worked particularly hard to increase cooperation with our European partners, to ensure that the EU speaks with one voice in the international arena.

The work of the EDPS is increasingly proactive, in recognition of the pace at which technological change now occurs. In 2016 we launched and developed new and interesting initiatives, designed to go beyond simple compliance with the rules and to confront some of the challenges faced by the data protection

community. These included the launch of the [Ethics Advisory Group](#) and the EDPS Accountability Initiative. We also continued to monitor new technologies, such as Artificial Intelligence, and turned our attention to preparing for new responsibilities, including the supervision of Europol and the establishment of the new EDPB.

Finally, within the Secretariat we improved the efficiency of our communication methods and continued to develop new tools to increase the transparency and accessibility of EDPS work. We also increased our administrative and financial efficiency, and initiated several projects designed to improve the working conditions of our staff (see Chapter 7).

### 4.1 RESPONDING TO NEW CHALLENGES

#### 4.1.1 Legislative reform

##### The countdown to the GDPR begins

On 4 May 2016 the [GDPR](#) was published in the Official Journal of the European Union. This marked the end of four years of intensive political discussions and negotiations and resulted in an ambitious and forward-thinking agreement which allows Europe to lead by example on the international stage.

In May 2018 the GDPR will take full effect. It will replace [Directive 95/46/EC](#), which pre-dates both the Lisbon Treaty, which elevated data protection to the status of a fundamental right, and the web-based economy. The GDPR assigns additional responsibilities to public authorities and private companies, including the need to appoint a [DPO](#).

In collaboration with the [WP29](#), the EDPS has invested substantial resources in preparations for the GDPR. Notably, we contributed to the drafting of guidance on key provisions of the GDPR for DPOs and on the one-stop-shop system (see section 4.5.3). Further work will take place in 2017 to ensure that both the new EDPB and the EDPS, which will provide the EDPB secretariat and be a member of the Board, are ready and operational when the GDPR becomes fully applicable (see section 4.5.5).



@EU\_EDPS

#GDPR rulebook will apply from 25 May 2018: let's prepare for it to strengthen rights of online generation #EUDatAP

### ePrivacy Directive under review

On 22 July 2016, the EDPS published an [Opinion](#) on the review of the ePrivacy Directive. It outlines the EDPS position on the key issues relating to the review and was carried out at the request of the European Commission.

Article 7 of the EU Charter of Fundamental Rights guarantees the confidentiality of communications between people. We share the view of the Commission that Europe needs a modern legal framework for ePrivacy that both protects this right and complements the protections offered by the GDPR.

Our Opinion emphasised the need for the new legal framework to be smarter, clearer and stronger and recommended that its scope be extended, both to match technological and societal changes and to ensure that individuals are afforded the same level of protection for all functionally equivalent services. The new rules should also continue to cover machine-to-machine communications, no matter what type of networks or communication services are used. We stressed that confidentiality must be protected on all publicly accessible networks and that user consent, when required, should be genuine, free and informed.

The EDPS will continue to monitor and contribute to the work on the revision of the ePrivacy Directive in 2017.

### Revising the Regulation

The reform of the EU data protection framework will also extend to [Regulation 45/2001](#), which applies to data processing operations carried out by EU institutions, agencies and bodies and sets out the role and responsibilities of the EDPS.

In 2015, we set up an informal working group, including a number of DPOs from the EU institutions, to share views on the revision of the Regulation, which will be

updated in line with the GDPR. Our discussions focused on [accountability](#) and the role of the DPO.

In April 2016 the working group submitted a report to the European Commission, comparing the provisions of the current Regulation with those of the GDPR and highlighting the provisions of Regulation 45/2001 that offer a higher level of protection than the GDPR. Our suggestions for the revised Regulation included retaining and moving to the main text the powers of the DPO, set forth in the Annex of Regulation 45/2001, and requiring that the DPO be consulted on the need for prior consultation related to a planned processing operation, to ensure that those responsible for processing the data concerned take the appropriate action.

### 4.1.2 Advising the EU institutions

In 2016, we advised the EU legislator on a number of high-profile topics related to data protection. These included the [Privacy Shield](#), negotiated by the Commission to replace the invalidated Safe Harbour decision in providing for the transfer of data between the EU and the US, and the [Umbrella agreement](#), designed to facilitate data transfers between the EU and the US for law enforcement purposes (see section 4.4.1). We also continued to follow the progress of EU trade agreements and their possible impact on the data protection rights of EU citizens, and provided advice on proposed legislation relating to EU border policy (see section 4.2).

The importance of the protection of fundamental rights within the EU continues to grow. It is therefore essential that the EDPS acts to consolidate its role as an advisor to the EU institutions, to ensure that the fundamental rights to privacy and data protection are upheld. This includes continuing to provide advice to the EU legislator on proposed legislation which has an impact on data protection, anticipating future developments and putting forward proposals to make it quicker and easier for policy makers to assess the impact of a proposal on data protection and privacy.

### The need to prove necessity

Articles 7 and 8 of the [EU Charter of Fundamental Rights](#) prohibit any action that might limit or interfere with the rights to data protection and privacy unless this action is proved necessary for an objective of general interest or to protect the rights and freedoms of others. Whenever a new proposal is under scrutiny, the question of necessity should be the first question addressed.

On 16 June 2016, the EDPS published for consultation a [background paper](#) on a necessity toolkit. We will use the feedback gained to develop the toolkit, which will help users to assess the necessity of measures that might interfere with fundamental rights, particularly those related to data protection.

One of the action points identified in the EDPS Strategy 2015-2019 is to help facilitate responsible and informed policymaking. With policy makers increasingly required to respond quickly to acute public security challenges, the need for help is greater than ever. Based on case law on the necessity principle issued by the Court of Justice of the EU and the European Court of Human Rights and on previous EDPS and WP29 Opinions on the subject, the toolkit will be designed for pragmatic use across all sectors of work. It will include an analysis of the main considerations involved as well as a checklist of criteria to be taken into account by the EU legislator when assessing the necessity of a draft measure.

A final version of the toolkit will be adopted in early 2017.



@EU\_EDPS

#EDPS issues background paper on #Necessity for stakeholder consultation #EUdataP #Privacy

### Data protection for finance

The EDPS was involved in a number of legislative projects in 2016 that aimed to improve accountability and transparency in financial markets. This included providing informal comments on:

- the Market Abuse Regulation (MAR), and the associated regulatory technical standards (RTS) and implementing technical standards (ITS);
- information exchange agreements concerning tax enforcement between the EU and third countries;
- new legislation on venture capital funds.

We also provided comments on the drafting of rules for the exchange of information on sanctions imposed by the authorities responsible for regulating financial markets.

On 5 July 2016, the Commission published a set of proposed amendments to the fourth Anti-Money Laundering [Directive \(EU\) 2015/849](#) and to [Directive 2009/101/EC](#), on the coordination of safeguards relating to EU companies. The amendments aim to reinforce the laws on anti-money laundering and terrorism financing whilst addressing tax evasion, in order to establish a fairer and more effective tax system. We have been following the legislative procedure, with a view to adopting formal comments or an Opinion on the topic in 2017.



### Cooperation on connected cars

Since 2015, the EDPS has contributed to the data protection sub-group of the European Commission's initiative on connected cars and Cooperative Intelligent Transport Systems (C-ITS).

C-ITS use information and communication technologies related to the road transport network to share information. Using these technologies, vehicles are capable of broadcasting or receiving data that allows them to communicate both with each other and the road transport infrastructure. The sub-group, known as WG4, aims to assess the issues related to privacy and data protection in C-ITS and provide recommendations to address them.

If C-ITS are to be fully compliant with data protection and privacy specifications, a thorough evaluation of their impact on user privacy is essential. The EDPS will therefore continue to contribute to the WG4 and monitor developments as this project progresses into 2017.



### 4.1.3 EDPS initiatives

#### Big plans for big data

The processing of personal information is indispensable for web-based services. However, it also enables them to covertly track the online activities of the individuals that use them. This is a problem not only because of the privacy implications involved, but also because it can allow companies with a dominant market position to gain an advantage, making it difficult for new competitors to emerge. As a result, market power and personal data is increasingly concentrated in fewer and fewer hands, making it harder for authorities to protect the rights and interests of individuals.

In our 2014 [Opinion](#) on privacy and competitiveness in the age of big data, we warned against EU rules on data protection, consumer protection and antitrust enforcement and merger control being applied in silos and called for a more holistic approach. On 23 September 2016, we published a second [Opinion](#), on the coherent enforcement of fundamental rights in the age of big data, in which we argued that the Commission's Digital Single Market Strategy presents an opportunity to implement such an approach.

In the Opinion we provided practical recommendations to the EU institutions on how to ensure that EU fundamental rights are respected. Specifically, we proposed the idea of establishing a Digital Clearing House, a voluntary network of regulators willing to share information and ideas on how to make sure web-based service providers are more accountable for their conduct.

On 29 September 2016, the EDPS, in collaboration with European consumer organisation BEUC, hosted a [conference](#) on the subject. The conference brought together leading regulators and experts in the competition, data protection and consumer protection spheres to discuss key areas of global economic and societal change,

to promote closer dialogue and cooperation among regulatory and enforcement bodies and to explore how to better respond to the challenges our society is facing.

We plan to set up the Digital Clearing House and continue our work on this topic in 2017.



@EU\_EDPS

New [#EDPS](#) Opinion calls for [#DigitalClearingHouse](#) for [#privacy](#) [#consumer](#) and [#competition](#) authorities [#BigDataRights](#)

#### Engaging with civil society

The second EDPS-Civil Society Summit took place on 16 June 2016. Participants discussed developments in legislation, such as the implementation of the GDPR, the directive on data protection rules for police and criminal justice and the review of the ePrivacy Directive. We also addressed recent case law, including the EU Court of Justice ruling on Safe Harbour and the proposed Privacy Shield agreement. We look forward to continuing and developing our cooperation with civil society groups in 2017.

## 4.2 EU BORDERS AND SECURITY

### 4.2.1 Securing Europe's rights and borders

The Commission proposed the European Border and Coast Guard Regulation in response to the ongoing migration crisis and the increased threat of terrorism in Europe. The Regulation aims to improve the management of external EU borders and involves transforming the EU's external border agency, Frontex, into a veritable European Border and Coast Guard.

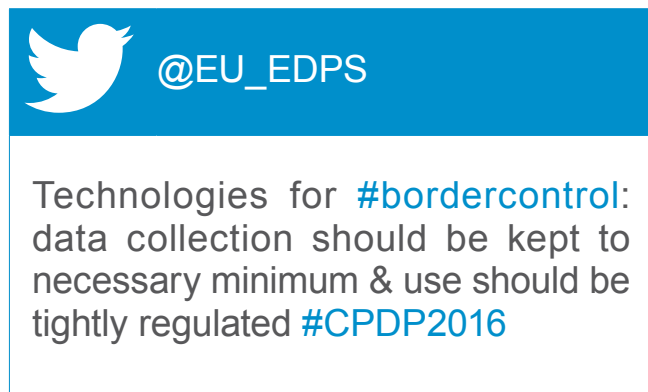
On 18 March 2016, we issued [recommendations](#) on the proposal. Whilst we acknowledged the urgent need for effective measures to deal with migration and combat cross-border crime, we also noted several concerns.

Migration and security are two very different problems. However, the proposed Regulation fails to deal with them as such. We therefore advised the Commission on the need to address the two areas separately,

particularly in terms of whether the proposed measures are both necessary and proportional to achieving the Commission's aims.

We also highlighted several points that required clarification. These included the scale and scope of the data processing activities to be carried out by the new European Border and Coast Guard Agency, the respective responsibilities of the new Agency and the relevant Member State agencies with regard to the processing of personal data, and the framework for transferring personal data to countries outside the EU and international organisations.

We stressed that respect for the fundamental rights of migrants and refugees must be a reality on the ground and that, to be able to exercise their rights, migrants and refugees need to know and understand them.



#### 4.2.2 Catching up with criminal records

ECRIS is a decentralised system that allows Member States to exchange information on convictions made by criminal courts in the EU. While the system works well when dealing with convictions relating to EU nationals, it is more difficult for authorities to exchange information on convictions concerning non-EU citizens.

To solve this problem, the European Commission proposed a decentralised system to process data relating to the criminal records of non-EU citizens. The system is based on a hit/no hit search feature, which would allow Member State authorities to search for an individual and identify which Member State holds details of their criminal convictions. Member States will therefore be able to see if an individual has previous convictions, but not to directly access their criminal record.

We issued an [Opinion](#) on the proposal on 13 April 2016. While we welcomed the idea, we identified three main areas of concern:

- the necessity and proportionality of collecting and storing the fingerprints of all convicted non-EU citizens, regardless of the crime committed;
- the necessity of using this system for EU nationals who are also nationals of a non-EU country;
- the claim that the data stored in the database would be anonymous when in fact it will only be pseudonymous, making it easier to identify the relevant individual.

#### 4.2.3 Smart Borders need smart policies

On 21 September 2016, we responded to the Commission's revised proposal to establish an Entry/Exit System (EES). The proposal aims to improve the management of EU borders by setting up a database to record the details of all non-EU citizens entering and exiting the EU.

In our [Opinion](#), we recognised the need for effective and coherent databases for border management and security purposes. However, we found that some of the proposed measures could interfere with the rights to privacy and data protection. These included:

- the proposed five year retention period for EES data;
- the collection of facial images for travellers requiring visas;
- the need for law enforcement authorities to access EES data;
- the requirement for individuals to provide fingerprints when exercising their rights of access to and correction and deletion of their personal data stored in the EES.



The EU already manages several [large-scale databases](#). We therefore recommended that the Commission assess the necessity and proportionality of what the EES system aims to achieve more broadly,



taking into account the purpose and capabilities of the databases already in operation. They should also ensure a clear distinction between data processed for border management purposes and data processed for law enforcement purposes, as both have a different impact on the rights to privacy and data protection.

#### 4.2.4 A Common European Asylum System that respects fundamental rights

The European Commission's first reform package on the Common European Asylum System proposes reform of the [Dublin Regulation](#), which determines the EU Member State responsible for examining applications for asylum, and the creation of a European Union Agency for Asylum.

On 21 September 2016, we published an [Opinion](#) on the package. We reminded the Commission that the unique identifier assigned to each asylum seeker in the Dublin database should not, under any circumstance, be used for purposes other than those described in the Dublin Regulation.



We also addressed proposed changes to the [Eurodac](#) system, a fingerprint database used in the asylum process. Specifically, we recommended that the Commission perform a full data protection and privacy impact assessment of the new proposals. We also advised them to assess the impact of the proposals on minors and to assess whether the collection and use of facial images is both necessary and proportional to achieving their aims.

#### 4.2.5 Bordering on privacy: EDPS continues work with Frontex

In 2015 we reported on our prior check Opinion on the use of personal data in risk analysis at Frontex (PeDRA). In 2016, Frontex was renamed the European Border and Coast Guard Agency and issued with a wider mandate, in an effort to help the Agency deal more effectively with the migration crisis. We remained in close contact with them throughout 2016, both to follow up on our Opinion and to provide advice on the data protection aspects of their new tasks.

The Agency hopes to use PeDRA to establish a hub for the collection of information on people smuggling. When their mandate changed in October 2016, they notified the EDPS of the implications of this for PeDRA. We issued an [Opinion on these changes](#) and will continue to work with the Agency to implement our recommendations.

We also issued an [Opinion on the legislative proposal](#) (see section 4.2.1) for the conversion of Frontex into the European Border and Coast Guard Agency. Among other things, we recommended ensuring a clear delineation of responsibilities between the Agency and Member States. We will stay in close contact with the Agency throughout 2017 to help them implement the changes brought about by the [new European Border and Coast Guard Regulation](#).

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

As part of its supervisory work, the EDPS has a duty to inspect the EU's [large-scale IT systems](#) on a regular basis. These are databases used by the EU to maintain control over its external borders. They allow national authorities and, in some cases, EU bodies, to exchange information related to borders, migration, customs, police, investigations and prosecution. The EDPS is responsible for supervising the central units of the system, while national [DPAs](#) supervise the national units, based in their respective countries.

In October 2016, we carried out the on-site part of our inspection of Eurodac, the European fingerprint database used to identify asylum seekers. We also followed up on an earlier inspection of the [Schengen Information System](#) (SIS), a database containing information on arrest warrants, missing person reports and stolen or lost passports. We will send our report on Eurodac, including our findings and recommendations, to the European Agency for the operational management of large-scale IT systems in the area of

freedom, security and justice (eu-LISA), which hosts the central unit of Eurodac, in 2017.

In summer 2016, we issued our inspection report for the most recent on-site inspection of the [Visa Information System \(VIS\)](#), which took place in autumn 2015. VIS deals with data submitted for short-term visa applications to visit the EU. We made several recommendations for improvement, all with specific deadlines, and will follow up on them with eu-LISA over the coming months.

Our supervisory tasks in this area are likely to increase in the near future as the EU is considering introducing several new databases. These include the EES (see section 4.2.3) and ETIAS, a travel authorisation programme for visa-exempt non-EU citizens.



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

In addition to our supervision of large-scale EU databases, the EDPS cooperates with national authorities to ensure consistency in the activities of the different supervisory authorities. National DPAs and the EDPS therefore meet regularly as part of distinct supervisory groups dedicated to each system. The EDPS acts both as a member of the groups, responsible for supervising the central unit of each database, based at eu-LISA and the European Commission, and as the Secretariat, in charge of organising the work of the groups under the authority of the Chair.

The [SIS II](#), [EURODAC](#) and [VIS](#) Supervision Coordination Groups met twice in 2016, in April and November. The [Customs Information System \(CIS\)](#) Supervision Coordination Group met on 9 December 2016. All groups adopted various reports aimed at better coordinating their supervisory activities and ensuring consistency in the approach of all supervisory authorities.

In 2016 a new visual identity was also adopted for each Supervision Coordination Group, including a [dedicated section](#) of the EDPS website, a logo and a specific colour scheme.

#### 4.2.8 Observing Schengen

In 2016, the European Commission invited staff members from the EDPS to participate as observers in the Schengen evaluation (SCHEVAL) of three Member States. The aim of SCHEVAL is to determine whether a Member State is correctly implementing the rights and obligations that apply to every state that participates in Schengen, known as the Schengen acquis.

The Schengen evaluation in the area of data protection assesses the independence, role and powers of the national DPA, data protection rules, including security, for the SIS and VIS databases, public awareness of Schengen and international cooperation. Where a Member State has not yet fully implemented the Schengen acquis, the aim is to assess whether they have met the necessary conditions to be able to apply it.

EDPS participation in SCHEVAL and our regular inspections and audits of the central SIS and VIS databases proved complementary tasks. Our experience was of clear added value in the supervision, enforcement and promotion of data protection rules in such a highly sensitive area. We look forward to further cooperation in the future.

#### 4.2.9 Security vs. Privacy: the encryption debate continues

The public debate on encryption intensified in 2016, with repeated calls from law enforcement and political representatives for restrictions on encryption, ways to break it or the weakening of encryption tools for consumers. The risks of such an approach for economy and society are significant: the integrity of encryption is necessary for the digital economy and for the protection of fundamental rights, such as privacy and free speech.

While there is no doubt that law enforcement must have the means to fight crime, including on the internet, any

new measure would have to pass the test for necessity and proportionality in advance, based on substantiated evidence. While encryption makes bulk data collection and mass surveillance difficult, it is not a limiting factor in more targeted measures.

The EDPS has promoted a clear and consistent message on encryption. In our [Opinion](#) on the reform of the ePrivacy Directive (see section 4.1.1), we stated that new rules on ePrivacy should protect the right to use encryption services in electronic communications without any interference from outside parties. EDPS Giovanni Buttarelli reinforced this message in 2016 in his speeches at the [Assemblée nationale française](#) and the [Coalition for Cybersecurity Policy and Law](#).

The debate is far from over, and the EDPS will continue to follow it closely whilst defending users' rights to privacy and data protection in electronic communication.



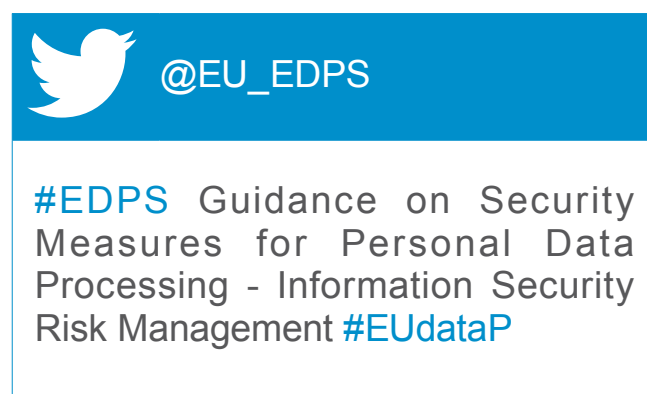
## 4.3 ON THE GROUND

### 4.3.1 The EDPS guide to securing information

In March 2016, the EDPS published a [Guidance document](#) explaining Article 22 of [Regulation 45/2001](#) and providing information on the steps EU institutions and bodies should take to comply with it. The guidance document is based on generally accepted good practices in Information Security Risk Management (ISRM). It aims to help EU institutions, as [controllers](#), responsible for processing personal data, to assume their responsibility according to the [accountability](#) principle.

Securing information is a key objective that any organisation must manage in order to fulfil its stated mission. Moreover, most organisations must deal with an ever-changing landscape affecting their operations.

Uncertainties created by such changes will affect how the organisation needs to react to ensure that its information assets are suitably protected. There is therefore a need for a specific framework that helps individuals responsible for information security to manage this. This framework is referred to as the ISRM process.



When processing personal data, risks must be mitigated as per the legal requirement stated in Article 22 of Regulation 45/2001. For this reason, it is integral that ISRM analysis covers information security risks affecting personal data and that, from this analysis, a set of suitable security measures are defined and implemented. The EDPS Guidance document helps the EU institutions to do this.

### 4.3.2 Protecting privacy in online communication

On 19 October 2016, the European Court of Justice [ruled](#) that, in many cases, the data collected by web servers, such as the [IP addresses](#) of users, is personal data. The decision underlined the need to put in place adequate safeguards to protect personal data when operating websites and other online services.

The EU institutions, and many other organisations, rely increasingly on online tools to communicate and interact with citizens. In addition, online transactions are becoming more complex. The implementation of effective data protection policies for the processing of all personal data used by web-based services is therefore essential to protect the rights of users. In particular, we need to address the use of cookies, online tracking, security and personal data transfers.

In November 2016, the EDPS published [Guidelines](#) on the protection of personal data processed through web services. The Guidelines offer practical advice to organisations on how to integrate data protection

principles into the development and management of their web-based services. They include recommendations on how to increase accountability, which requires that organisations not only comply with data protection rules but are also able to demonstrate their compliance.

The Guidelines take into account input from relevant experts at the EU institutions and agencies. They also incorporate feedback from the [DPOs](#) of the EU institutions, who are responsible for ensuring that their respective organisations comply with data protection rules.

### 4.3.3 Guidelines for going mobile

In November 2016, the EDPS published [Guidelines](#) offering practical advice to organisations on how to integrate data protection principles into the processing of personal data by mobile applications.

Mobile apps are software applications used on smart devices, such as smartphones and tablets. Most of them are designed to interact in a specific way with a wide range of online resources and can also exchange information with other connected devices. The tools integrated into smart mobile devices, such as cameras, microphones and location detectors, are also often exploited by apps. However, though these tools increase the value of an app for users, their use may involve the collection of great quantities of personal data.

Our Guidelines provide advice on how to ensure that mobile apps process this data in a way that does not interfere with an individual's privacy.



### 4.3.4 Whistleblowing in the EU institutions

The [EU Staff Regulations](#) mandate that all EU institutions and bodies must have clear whistleblowing procedures in place. All EU employees are also required to report immediately any activity that might be

considered illegal. However, many people are reluctant to report such behaviour due to a fear of retaliation.

On 18 July 2016, the EDPS published [Guidelines](#) on the processing of personal information as part of a whistleblowing procedure. These Guidelines are designed to help EU institutions and bodies prepare and implement their whistleblowing procedures in a way that complies with data protection principles. Addressing whistleblowing procedures in EU institutions prior to any investigation by the European Anti-Fraud Office (OLAF), the Guidelines provide recommendations on how to create safe channels for staff to report fraud, to ensure the confidentiality of information received and to protect the identities of the whistleblower, the alleged wrongdoer and anyone else connected to the case.

The Guidelines build on years of practical experience, gained through our supervision work and our work on previous EDPS decisions and Opinions. They also take into account feedback from DPOs to ensure that they work effectively in practice.

A Twitter social media graphic for @EU\_EDPS. It features the Twitter bird logo and the handle @EU\_EDPS. Below this, the text reads: #DataProtection and #Whistleblowing in the #EUInstitutions - #EDPS guidelines.

### 4.3.5 Dealing with rule-breakers in the EU institutions

In November 2016 we published revised [Guidelines](#) on the processing of personal information in administrative inquiries and disciplinary proceedings. The Guidelines provide advice to the EU institutions on how to prepare and implement appropriate procedures in administrative inquiries or disciplinary proceedings and ensure that the processing of personal data complies with [EU data protection rules](#).

Though the EU Staff Regulations set out the legal basis required for disciplinary proceedings, they do not provide a sufficiently detailed legal basis for the conduct of administrative inquiries. The EDPS Guidelines aim to fill this gap, by providing the EU institutions with an adequate framework. Most importantly, they ensure that EU institutions and their

investigators are able to prepare and implement their procedures in a way that ensures the processing of personal data is lawful, fair and transparent and complies with their data protection obligations.

To launch an administrative inquiry into a breach of the Staff Regulations, an EU institution must adopt a specific legal instrument, such as a legally binding decision, policy or implementing rules. Investigators should choose the least intrusive means possible to collect data, taking into account the principles of necessity and proportionality. The person under investigation and all individuals involved in an inquiry should be aware of their data protection rights and how to exercise them.

The [EDPS Strategy 2015-2019](#) outlines the importance of increasing the [accountability](#) of EU institutions with regard to data protection. In practice, this means helping them not only to comply with EU data protection rules, but to be able to demonstrate their compliance. [EDPS Guidelines](#) support them in this by providing practical advice and serving as a reference document against which organisations can measure their activities.

Though our Guidelines are aimed at the EU institutions, they are often also useful for, and can be applied to, the work of other organisations.

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

The EDPS meets with the DPOs of the EU institutions and bodies twice a year. In 2016, these meetings took place in April and October and were hosted by Eurofound in Dublin and the European Union Intellectual Property Office (EUIPO) in Alicante. The meetings are a chance for us to interact with our data protection partners and reinforce our collaboration.

Following the success of the 2015 meetings, we continued to organise discussions in the form of interactive workshops. In Dublin we focused on the EDPS [eCommunications Guidelines](#), staff appraisals, whistleblowing and cloud computing. In Alicante we addressed the right of access, EDPS Guidelines on [mobile applications](#) and [web services](#), and [Data Protection Impact Assessments](#). For new DPOs, we

also ran a workshop on the practical application of [Regulation 45/2001](#).



Under the [GDPR](#), which will be fully applicable from May 2018, public authorities and some private companies will be required to appoint a DPO. Drawing on our experience of working with DPOs in the EU institutions, the EDPS worked as co-rapporteur in the [WP29](#) subgroup responsible for preparing [DPO Guidelines](#). The Guidelines were adopted in December 2016 and we hope that they will help organisations in the public and private sector to better prepare for the new rules.

#### 4.3.7 A privacy-friendly cloud?

Cloud computing is becoming an increasingly appealing tool for many EU institutions, allowing them to cut ICT costs and increase productivity. However, the introduction of cloud technology also raises complex issues for data protection. The EDPS has been working with the EU institutions to ensure that the benefits of cloud technology can be enjoyed without compromising the right to data protection.

At the DPO meeting in Dublin, on 28 April 2016 (see section 4.3.6), we conducted interactive workshops on cloud computing. DPOs were able to discuss and receive advice on how to decide whether a cloud solution was appropriate for their institution and the data protection safeguards required to implement it.

The EDPS also provided advice to several EU institutions on the adoption and use of cloud services. When consulted, we evaluated each case separately and issued recommendations where necessary, focusing on the specific risks the proposed cloud service might pose to the rights and freedoms of the individuals concerned.

As part of our active support for the work of the International Committee of the Red Cross (ICRC), and other international organisations, on the protection of personal data, on 28 September 2016 we participated in a dedicated workshop on cloud services, organised by ICRC and the Brussels Privacy Hub. We reported on the supervision and policy experience of the EDPS, with specific reference to the idea of a *model cloud agreement*. Our advice focused on a *data protection strategy for cloud*, in which we outlined the various steps involved in adopting cloud services, including assessment of the cloud computing option, contracting the cloud service and maintenance and dismissal of the service.

We aim to finalise Guidelines for the EU institutions on the use of cloud computing in 2017, incorporating the feedback and knowledge we have gained through our work on this topic.



#### 4.3.8 A Reference Library for data protection

As outlined in the [EDPS Strategy 2015-2019](#), we consider it vital to make data protection easier, clearer and less bureaucratic. With this in mind, in January 2016 the EDPS launched a [Data Protection Reference Library](#). The virtual library includes a range of subjects related to EDPS supervision of the EU institutions and bodies. Each section of the Library includes key points about the subject in an easy-to-read style, as well as links to relevant documents issued by the EDPS.

The aim of the Reference Library is to share our expertise with the EU institutions and support them in integrating data protection principles into their everyday work. However, the library is also relevant and accessible for a wider audience. It is updated regularly and new subjects will be added over time.

#### 4.3.9 Protecting privacy in the EU institutions

##### The right to information

The EDPS dealt with several complaints in 2016 relating to the right of individuals to be properly informed of the processing of their data. One of these concerned an internal mobility exercise. An EU institution transferred the CV of an employee to services other than those with vacant posts in which the employee had expressed an interest. The employee argued that these services did not qualify as recipients of his personal data and that the institution had not properly informed him that such a transfer might take place.

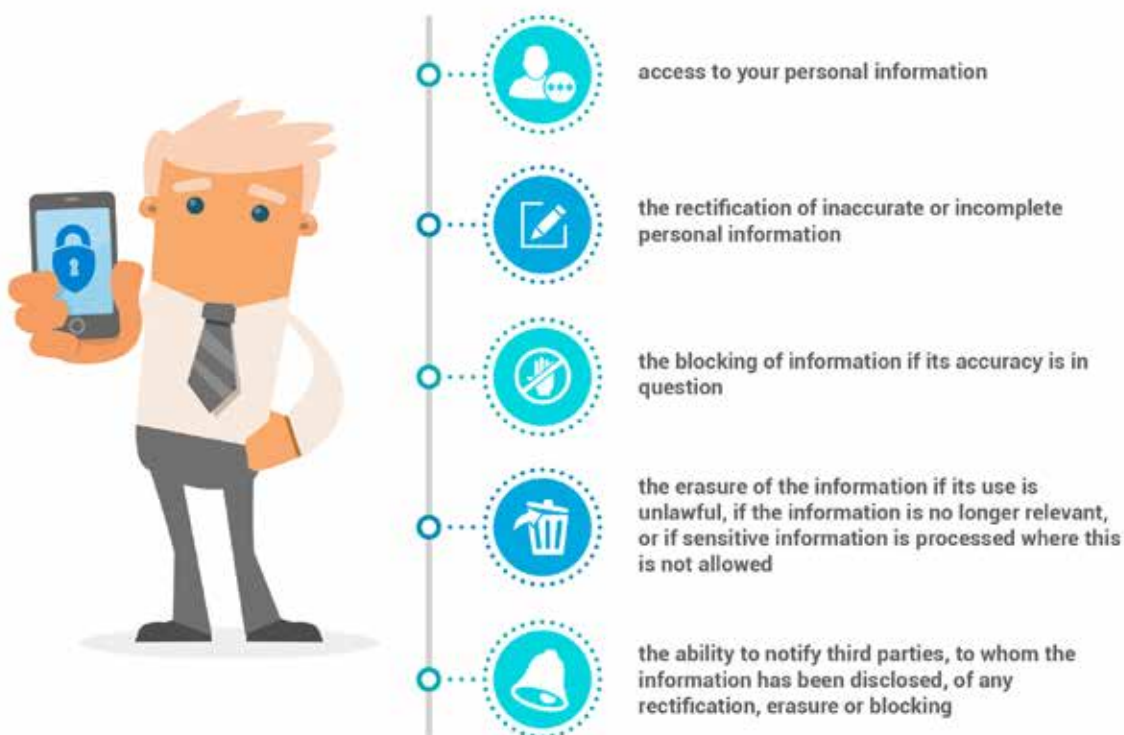


#### Commission's Cloud I gets off the ground

The first inter-institutional Call for Tender for the provision of cloud-based IT services (Cloud I) was initiated in 2016. A subgroup of the Cloud Virtual Task Force (CVTF), launched by the European Commission's Directorate General for Informatics (DG DIGIT) as part of their cloud strategy, will monitor the security and data protection controls offered by the prospective contractors.

The EDPS has actively contributed to raising awareness amongst participating EU institutions on how best to protect personal data when using cloud services. We have also further defined requirements for compliance with the [data protection rules](#) which apply to the EU institutions and helped to prepare for the changes that will come with the reform of these rules, to be finalised in 2017.

You are entitled to check any information being processed that is related to you and obtain, free of charge:



You can object at any time, on compelling and legitimate grounds, to the processing of your personal information.

We found that while the actions of the EU institution complied with the requirements of data protection rules, the institution had not respected data protection principles relating to data quality, most specifically the right to receive clear information on the processing of personal data. Though a data protection notice was available, warning that personal data might be processed in this manner, it was only published on the webpage of the institution’s DPO and not on the relevant page of the institution’s website.

The EDPS decision noted that the institution had already taken measures to address the lack of information. We recommended, for the sake of clarity and fairness, that the institution revise the data protection notice and publish the new version without further delay, ensuring that it is readily accessible and included in the essential information provided to employees about the internal mobility exercise.

**The right to be forgotten**

In 2016, the EDPS successfully closed a complaint case relating to the publication of the name of a

candidate who had passed a European Personnel Selection Office (EPSO) competition to become an EU official. When requesting the removal of his name from the relevant list, published in the Official Journal of the EU, the individual put forward convincing arguments related to his personal circumstances. After consulting with the EU Publications Office, EPSO confirmed that the individual’s name had been removed from the list.

**The right to privacy**

In another case, an individual claimed that her employer, an EU Agency, breached the privacy of her correspondence. A letter sent to her from another EU institution was opened and read by unauthorised staff working at the Ministry of Interior of the country in which her employer is located.

An agreement between the EU institution and the relevant Ministry of Interior states that all mail addressed to the Agency which does not indicate that it is private or confidential will be opened for registration and business continuity purposes. This

policy, however, was officially adopted three weeks after the incident took place.

The EDPS found that the employer had contravened the [rules](#) governing data protection practice in the EU institutions. This was because no legal basis existed for the Ministry staff to open and read the letter. We also found that the Agency failed to adequately inform all staff about the correspondence policy of the institution.

We used similar arguments in an important case relating to the issue of private correspondence at the European Court of Human Rights. We strengthened our case by referring to Article 7 of the [EU Charter of Fundamental Rights](#) and Article 8 of the [European Convention on Human Rights](#), which guarantee the right to privacy of correspondence, and to the importance of the adoption of a policy on correspondence.

#### The right to erasure

We dealt with several complaints in 2016 concerning the erasure of personal data by EPSO. These related to individuals who no longer wished to pursue a career in the EU institutions and therefore requested that EPSO delete their data and accounts. EPSO refused to do this, citing the data conservation periods established and approved by the EDPS.

We agreed that in competitions which were still ongoing, EPSO was entitled to retain the complainants' personal data, in the interest of fairness of competition and in case of possible reviews. However, we suggested separating the conservation periods for different competitions, so that older competitions could disappear from the system, even if the person concerned participated in other competitions in the future.

#### Making exceptions

In one case, an individual contested the fact that she was denied access to the full text of a letter concerning her previous professional activities.

In our decision of 26 August 2016, we acknowledged that the letter constituted personal data relating to the individual. However, we also noted that there was no express and legitimate reason for full disclosure of the letter and that the author of the letter objected to disclosing his name. We therefore concluded that the Commission evaluated and responded correctly to this request for access to personal data.

One of the main duties of the EDPS, as established by [Regulation \(EC\) No 45/2001](#), is to *hear and investigate complaints* as well as *to conduct inquiries either on his or her own initiative or on the basis of a complaint* (Article 46).

In 2016, the EDPS received 173 complaints, an increase of approximately 20.98% compared to 2015. Of these, 145 complaints were inadmissible, the majority relating to the processing of personal data at national level as opposed to processing by an EU institution or body.

The remaining 28 complaints required in-depth inquiry. In addition, 47 cases submitted in previous years were still in the inquiry, review or follow-up phase on 31 December 2015 (two in 2012, four in 2013, 15 in 2014 and 26 in 2015). In 2016 we issued 22 complaint decisions.

#### 4.3.10 Transparency vs. protection of personal data

##### Striking a balance

On 8 December 2015, the EDPS responded to a complaint relating to the publication of a European Ombudsman (EO) inquiry into alleged maladministration by the European Commission in the assessment of conflict of interests.

Our response established the conditions and limits for the processing and publication of the complainant's personal data. This included:

- instructing the EO to refrain from publishing any of the complainant's personal data in their preliminary conclusions;
- instructing the EO to replace the reference to the complainant's full name with a reference to her appointment in the publication of the decision on the EO inquiry.

Our guidance aimed to strike a balance between transparency, as sought by the EO, and the right to the protection of personal data, as sought by the individual concerned.



## Number of complaints received

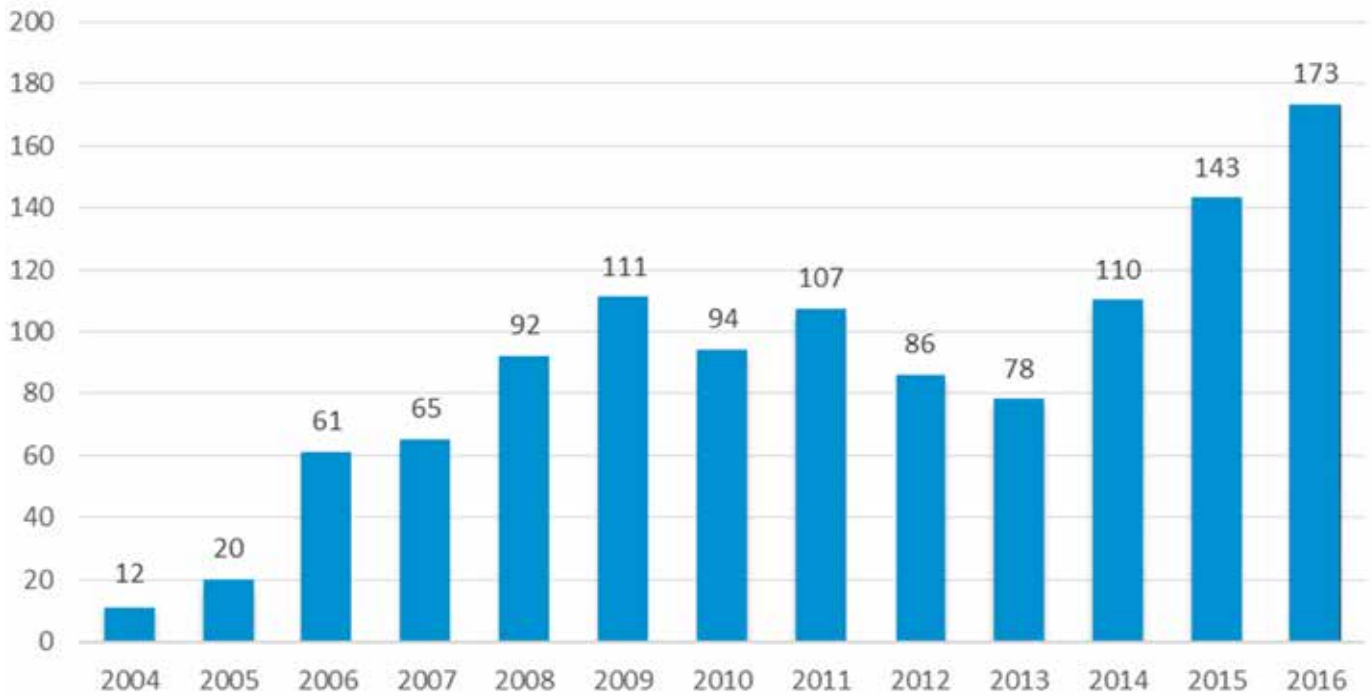


Figure 2. Evolution of the number of complaints received by EDPS

## EU institutions and bodies concerned 2016

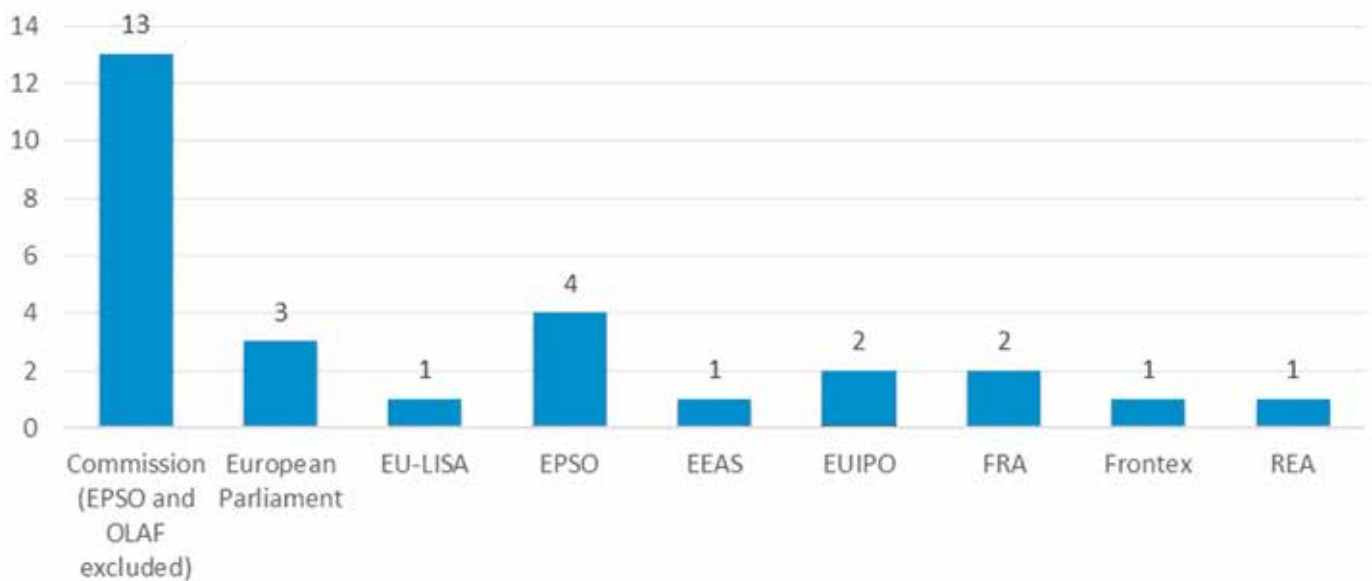


Figure 3. EU institutions and bodies concerned by complaints received by EDPS

## Topics of complaints 2016

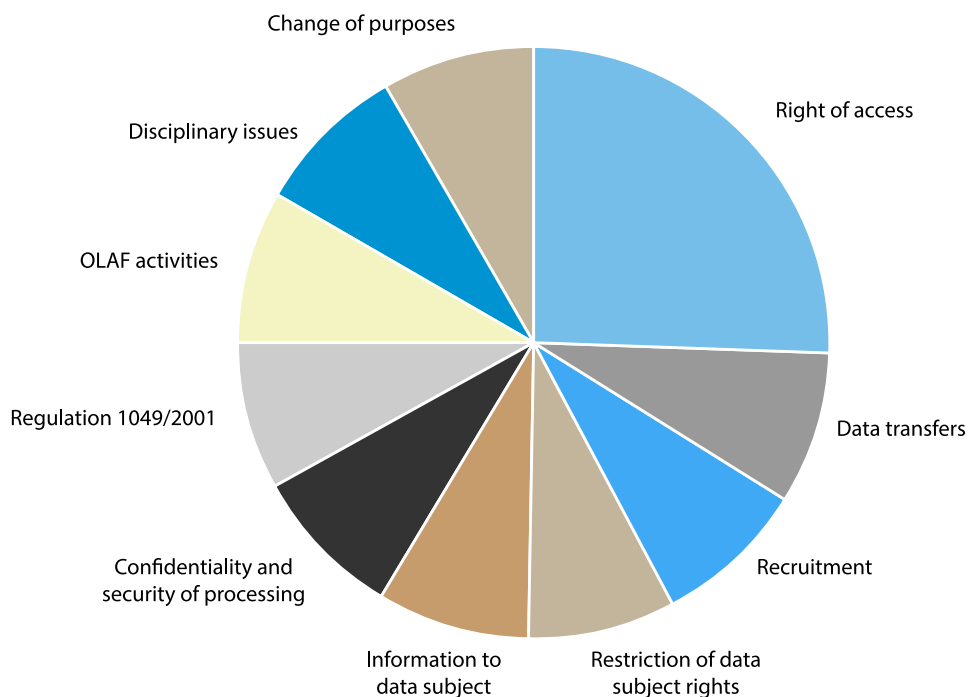


Figure 4. Type of violation alleged in complaints received by EDPS

Unhappy with this decision, on 26 May and 2 June 2016, the complainant initiated judicial proceedings, requesting firstly the annulment of the EDPS decision and, secondly, interim measures against the EDPS before the General Court of the European Union.

In our defence, we argued that the EDPS decision was a reasonable solution, consistent with EDPS practice on this issue. We also explained that referring to a broader description of the individual in question could affect the interests of other individuals who might fall under a similar description, and that the individual concerned was a public figure, whose position was investigated by the EO in relation to the conditions the complainant had to comply with to assume their political mandate.

In view of these arguments, the case was dropped on 5 August 2016, leaving the EDPS decision in place as a valid demonstration of how to balance the need for both transparency and data protection.

### Publishing transparently

The European Forum of Official Gazettes is an annual gathering involving the Publications Office (PO) of the European Union and other *official publishers* from the

EU Member States. It took place at the Austrian Ministry of Justice in Vienna on 15-16 September 2016.

The Forum is an opportunity for publishers to discuss the publication process, technology and best practice. As part of the 2016 Forum, we were invited to share our experience on ensuring compliance with data protection rules whilst preserving transparency in official publications produced by EU institutions and bodies.

Similarly, on 12 December 2016, the EDPS was invited to give a presentation to an Expert Group set up by the [EU Council Working Party on e-Law](#). The Group aims to issue guidelines on official publications and data protection, with the objective of harmonising as far as possible EU and national practices.

In our presentation, we referred to our experience on this matter, which includes past cases relating to asset freezing at the Council and the European External Action Service (EEAS), the publication of petitions and written declarations by the European Parliament and of decisions by the European Ombudsman and *transparency publications* issued by EU institutions and agencies.

In collaboration with the EDPS, the Group has drafted a questionnaire on the topic addressed to competent national authorities. Replies to the questionnaire are expected in the first half of 2017 and draft guidelines should be finalised and sent to the Working Party on e-Law for approval by the second half of 2017. We hope that these guidelines will reflect an appropriate balance between the need for transparency and the need for data protection and therefore serve as a useful reference tool for EU publishers.

#### 4.3.11 Data protection for social workers

On 11 January 2016 we replied to a request for consultation from a social worker at an EU Agency, concerning the disclosure of personal data.

We advised that, in compliance with the confidentiality duties to which social workers and psychologists are bound, information relating to individuals who use their services cannot be disclosed, except when necessary to protect the vital interests of the individual concerned. This non-disclosure obligation should be stated in a data protection notice, which must be given to any staff member making use of the service.

In line with previous EDPS opinions on the matter, we noted that in exceptional cases the social worker may disclose personal information, but only that which is strictly necessary to achieve the purpose of the data processing and which complies with the regulations applicable to the specific EU Agency. Reports made by the social worker to their hierarchy must only contain statistics about the activities they carry out.

If a DPO has any doubts about the need for prior checking, they must consult the EDPS. We determine whether or not the proposed data processing presents specific risks and requires the detailed analysis of a prior check.

In 2016, we received 55 consultations on administrative measures. We issued 25 formal consultative opinions in addition to providing advice at staff level.

#### 4.3.12 A healthy approach to data protection

##### Hope for rare diseases

All EU citizens and individuals residing in the EU with congenital anomalies or cerebral palsy may enrol in

their local, regional or national registries and provide details about their health. The Joint Research Centre (JRC) aims to use this information for research on how to reduce mortality rates, anomalies, impairment and disabilities, improving quality of life and promoting best practice in prevention and care for EU citizens.

However, individuals whose information is included in these databases are indirectly identifiable. The EDPS therefore stressed the need for the JRC to adopt a delegated act or alternative measure to establish the lawfulness of the processing of health data in this particular case. We also advised them to prepare a data protection notice, and ensure that it is provided to all participants, and to determine a maximum retention period for the data collected.

##### Disability and data protection

The Equal Opportunities Office of the Council of the European Union produces videos, posters and other materials on the workplace experiences of individuals with disabilities. Their aim is to promote non-discrimination. However, the activities involved require the processing of personal information, including sensitive health data.

We reminded the Equal Opportunities Office that the consent of the individuals participating in the initiative is required in such cases. Moreover, when relying on consent in the workplace, it is vital to ensure that this consent is free and informed. We therefore recommended that a data protection notice be published on the institution's intranet. This should also be given to staff members, alongside the consent form, prior to their participation in the activities of the Equal Opportunities Office. The consent form and the data protection notice must also specify that the decision on whether to give consent will not prejudice any individual rights or interests at work.

Regulation (EC) No 45/2001 provides that 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 are to be subject to prior checking by the EDPS (Article 27(1)).

In 2016, we received 65 notifications for prior checking, the same number as in 2015. We issued 52 prior check Opinions, a decrease of approximately 22.3% from 2015.

Of these, one was a joint opinion covering three notifications and four were updated Opinions following updated notifications. We also issued six non prior check Opinions, as well as six consultations on the need for prior checking.

85% of the risky processing operations we were notified about in 2016 related to administrative procedures, such as recruitment of staff, their annual appraisal or the conduct of administrative inquiries and disciplinary procedures, as has been the trend in past years. However, in 2016 we also witnessed an increase in the number of notifications about core business activities.



### Notifications to the EDPS

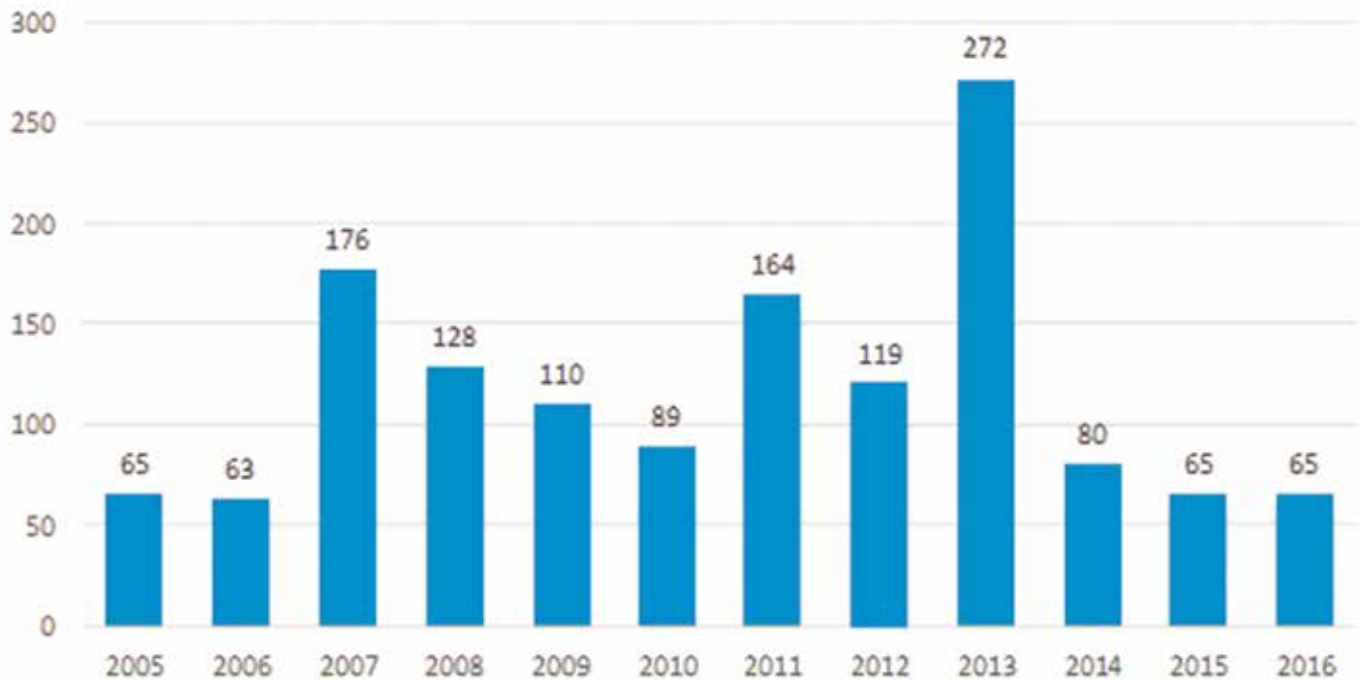


Figure 5. Evolution of Notifications received by EDPS

### EDPS prior check Opinions per year

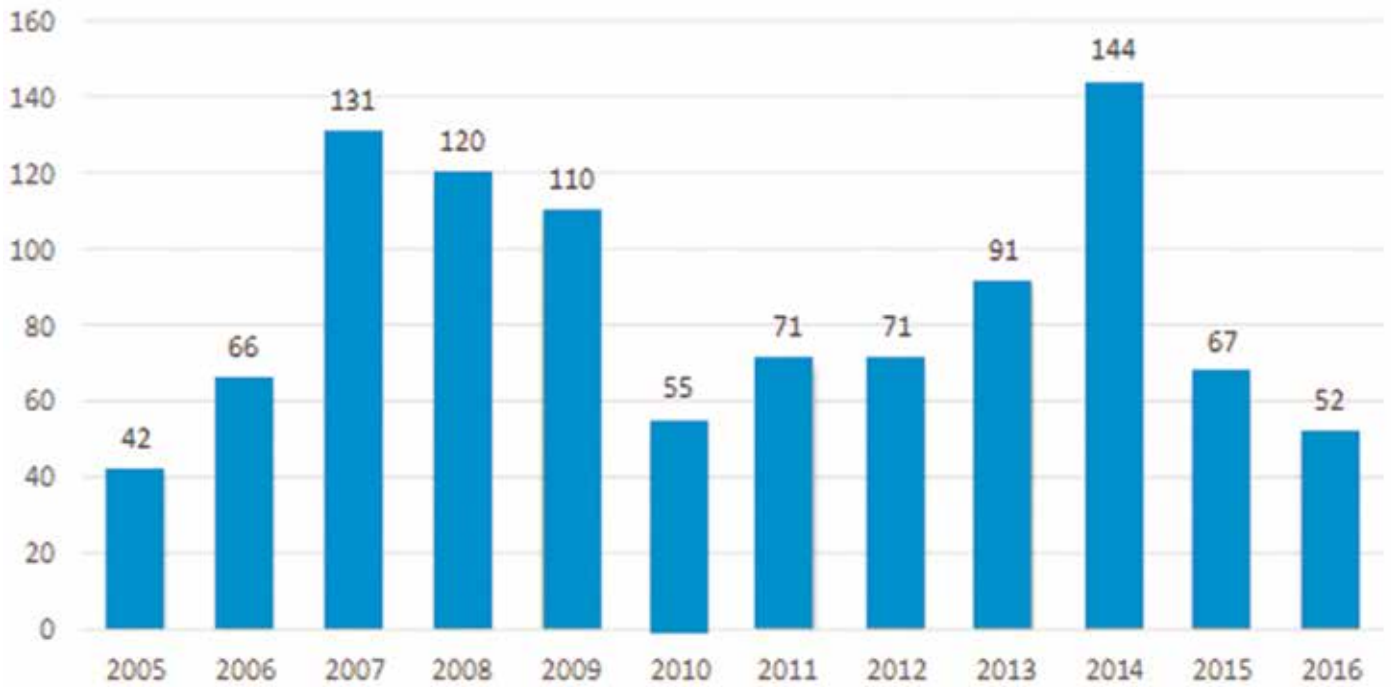


Figure 6. Evolution of prior check Opinions issued by EDPS

### Notifications to the EDPS 2016 Core Business vs Administration

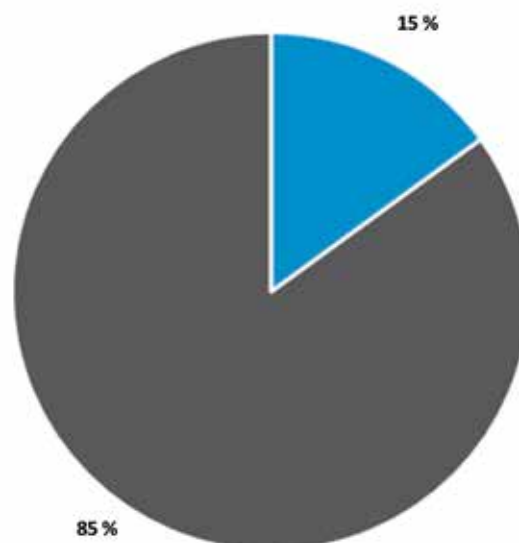


Figure 7. Percentage split between Core Business and Administration activities in the Notifications received by EDPS

### 4.3.13 Partners in compliance

In line with our Strategy objective to strengthen links with our stakeholders, two secondments took place during the first half of 2016. These involved two members of the EDPS Supervision and Enforcement Unit, one working with the European External Action Service (EEAS) and the other with the European Securities and Markets Authority (ESMA).

The aim of these secondments was to support the development of a data protection culture within the concerned EU bodies and provide practical guidance to the DPOs working there. The seconded EDPS staff members held meetings with relevant [controllers](#) and members of staff in the different units to help them with pending notifications and to advise them on topics such as data retention and transfers. At the EEAS, work also focused on ongoing efforts to implement data protection rules in the 139 EU delegations around the world.

The secondments were useful for both the hosting institution and the EDPS. We gained a better understanding of their tasks and responsibilities and the challenges they face in complying with data protection rules, whilst helping them to improve their data protection awareness and establishing the EDPS as a partner in their journey towards full data protection compliance.

### 4.3.14 Catching up with the institutions: inspections and visits

In 2016, we undertook four [inspections](#). Inspections are one of the tools used by the EDPS to ensure that the EU institutions comply with the rules set out in Regulation 45/2001.

One of these inspections involved a fraud prevention database, known as *Arachne*, at the European Commission's Directorate General for Employment, Social Affairs and Inclusion (DG EMPL). The risk scores identified by Arachne are used to select targets for audit. As auditing the wrong target because of incorrect information could lead to invasion of an individual's privacy and to the misallocation of audit resources, it is essential that the information contained in Arachne is correct, up-to-date and necessary for the purpose specified.

Another inspection, at the European Defence Agency (EDA), covered the implementation of retention periods and access control issues. We selected the EDA as an inspection target based on a revised version of our risk assessment exercise, which we use to establish our annual inspection plan.

We also inspected Eurodac, the EU's database for processing asylum requests, in line with our obligation

to carry out inspections on this and other [EU large-scale IT systems](#) on a regular basis (see section 4.2.6), and Sysper2, the Human Resources Management information database operated by the Commission's Directorate General for Informatics (DG DIGIT).

In addition to inspections, we carried out an unprecedented number of visits in 2016. This included seven accountability visits (see section 4.5.1) and four compliance visits. Compliance visits are used in EU institutions where our monitoring activities show a lack of commitment to data protection. They involve an on-site visit by the EDPS or Assistant Supervisor and ensure results through a mutually agreed road map and increased awareness of data protection issues at all levels of management. In 2016 we carried out compliance visits to Fusion for Energy (F4E), the EU Intellectual Property Office (EUIPO), the European Institute of Innovation and Technology (EIT) and the European Investment Fund (EIF).

Inspections are one of several tools used by the EDPS to monitor and ensure the application of [Regulation 45/2001](#). Articles 41(2), 46(c) and 47(2) give the EDPS extensive powers to access any information, including personal data, necessary for his inquiries and the right to access any premises where the [controller](#) of the EU institution or body carries out its activity. Article 30 of the Regulation requires EU institutions and bodies to cooperate with the EDPS in performing his duties. The [2013 EDPS Inspection Guidelines](#) contain the criteria the EDPS applies to launch an inspection and a [2013 Policy Paper](#) on inspections further explains the EDPS' approach to inspections.

## 4.4 INTERNATIONAL COOPERATION

### 4.4.1 International data transfers

#### No Safe Harbour for the EU institutions

In 2015 we reported on the [invalidation of the Safe Harbour decision](#) by the EU Court of Justice (CJEU). In 2016, we received the results of a survey we launched shortly after the ruling. It revealed that various transfers of personal data from EU institutions and bodies to the US were carried out using the Safe Harbour decision. Most of these involved service providers, web-based services or internet platforms, including social media.

The EDPS received several requests for consultations from EU [DPOs](#) relating to the ruling. Our replies reiterated that, following the Court decision, it is no longer permitted to transfer data from the EU to the US using Safe Harbour. We also reminded DPOs of the alternative tools available to perform these transactions, including [Standard Contractual Clauses](#) (SCCs) and [Binding Corporate Rules](#) (BCRs) and referred them to the [WP29 statement](#) on the issue. However, we stressed that though SCCs and BCRs were not affected by the Safe Harbour ruling, they should be used cautiously.

In the days following the CJEU judgement, the EDPS received a complaint from an EU citizen. The complaint concerned the use by an EU institution of a service provider using Safe Harbour to transfer data to the US. The complainant argued that such transfers no longer had any legal basis and should be stopped. Our investigation into the complaint is ongoing.

#### Privacy Shield must provide more protection

To replace the invalidated Safe Harbour decision, the European Commission proposed the [EU-US Privacy Shield](#), designed to provide a more robust framework for the transfer of personal data from the EU to the US.

The EDPS issued an [Opinion](#) on the Privacy Shield on 30 May 2016. Though we welcomed the effort made to develop a suitable replacement for Safe Harbour, we concluded that the improvements proposed in the new framework were not sufficient. Our Opinion also took into consideration the new [GDPR](#) and the need to fully respect EU law as interpreted by the CJEU judgement on Safe Harbour.



We recommended strengthening the main principles of this new self-certification system, including the provisions on data retention, purpose limitation and the rights of individuals. We also called for robust safeguards

regarding access to personal data by US public authorities, improved oversight and redress mechanisms and less scope for exemptions from the law.

#### Umbrella Agreement requires further clarification

In February 2016, the EDPS issued an [Opinion](#) on the EU-US umbrella agreement. The agreement concerns the protection of personal data transferred for law enforcement purposes.



We welcomed the efforts of the European Commission to conclude a sustainable arrangement in this area, but recommended three essential improvements to ensure compliance with the [EU Charter of Fundamental Rights](#) and Article 16 of the Treaty on the Functioning of the EU, which protect the rights to privacy and data protection. Our recommendations included:

- clarifying that all safeguards in the agreement apply to all individuals, not only to EU nationals;
- ensuring that provisions relating to the right to judicial redress are in line with the Charter;
- clarifying that transfers of sensitive data in bulk are not authorised.

#### 4.4.2 International cooperation

The EDPS continued to develop our international activities and networks in 2016, in line with the objectives outlined in our [Strategy 2015-2019](#). In addition to our work with national [DPAs](#), we improved our cooperation with international partners in an effort to develop cross-border, coordinated approaches that protect the rights of individuals wherever they are in the world.

### Article 29 Working Party

The WP29 is composed of representatives from the national DPAs of the EU Member States, the EDPS and the European Commission. Its main tasks are:

- to provide expert advice to the European Commission on data protection matters;
- to promote the uniform application of [data protection law](#) in all EU Member States, as well as in Norway, Liechtenstein and Iceland;
- to advise the Commission on any EU law that affects the right to the protection of personal data.

In 2016 the EDPS participated in several WP29 subgroups including those on technology, international transfers, eGovernment, Borders Travel and Law Enforcement (BTLE) and financial matters. We also participated in subgroups working on the future of privacy and key provisions, dedicated to preparations for the introduction of the GDPR (see sections 4.1.1 and 4.5.3).

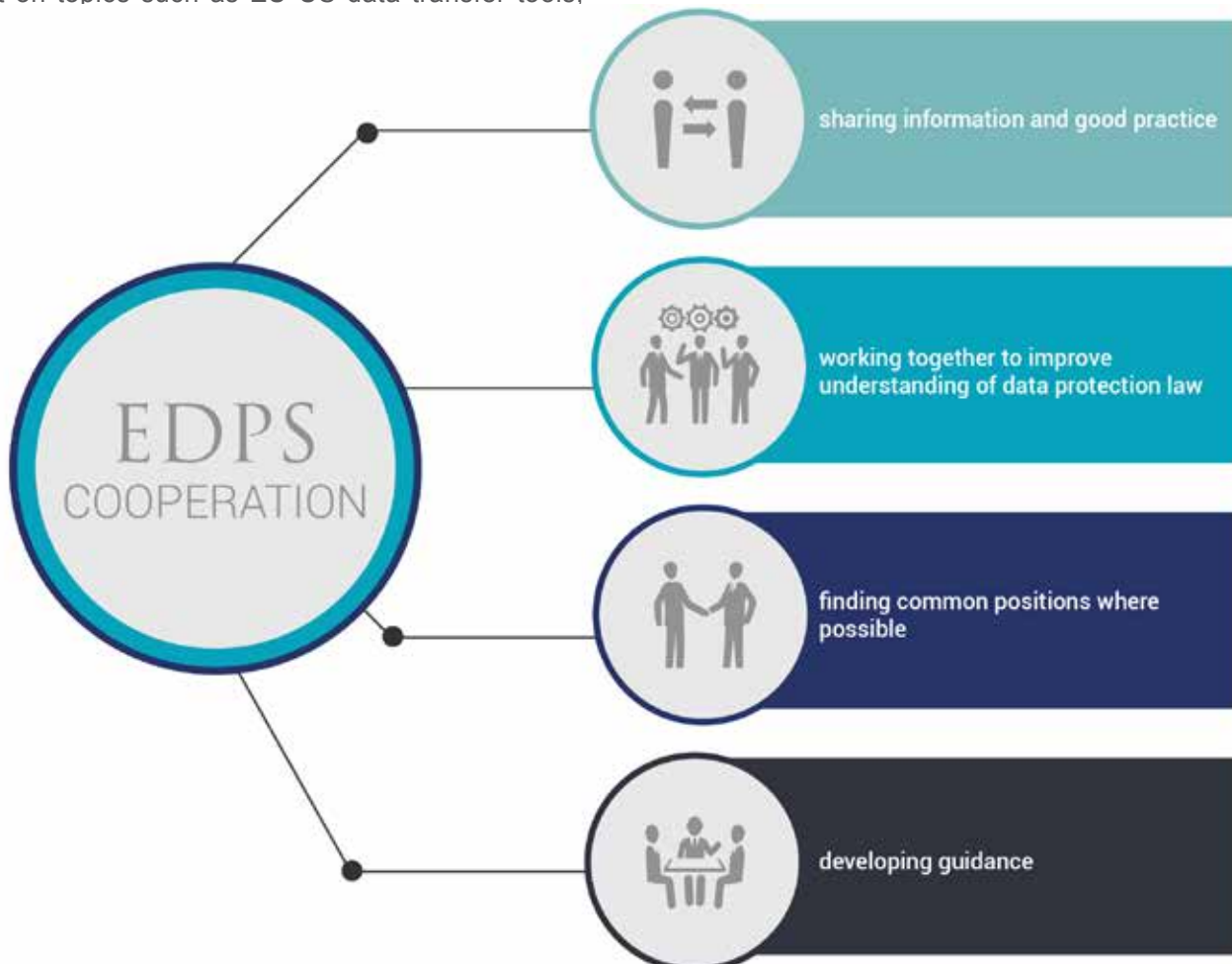
In addition to our work in the subgroups, we provided input on topics such as EU-US data transfer tools,

including the umbrella agreement and privacy shield, border controls, money laundering, ePrivacy, and [data protection impact assessments](#). Our work with the WP29 will continue and intensify in 2017 as the deadline for the GDPR draws closer.

### Council of Europe

The Council of Europe is an important player in privacy and data protection law and policy, not only in Europe but across the world. Any country can sign up to the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

The EDPS, as an EU institution, is an observer in the Council of Europe’s expert groups on data protection, including the Consultative Committee (T-PD) of Convention 108 and the ad-hoc Committee on Data Protection (CAHDATA), entrusted with the modernisation of Convention 108. We attend the meetings of these expert groups and provide informal comments, with a view to ensuring a good level of data protection and compatibility with EU data protection standards.





In 2016, the EDPS continued to contribute to the modernisation of Convention 108, providing written comments on the review of the Convention and its explanatory report and attending CAHDATA meetings where necessary. In T-PD meetings, we make particular contributions to discussions on guidelines and opinions relating to big data, [Passenger Name Records](#) (PNR), police data and health data.



## OECD

The EDPS follows the OECD Working Party on Security and Privacy in the Digital Economy as an observer. We advise the European Commission where necessary and provide comments on recommendations relating to the protection of privacy and data protection. In 2016, we provided advice on the OECD Council Recommendation on Health Data Governance.

## The International Conference

Marrakech, Morocco was the location of the [2016 International Conference of Data Protection and Privacy Commissioners](#). The main topic of discussion in the closed session was the implications of Artificial Intelligence, machine learning and robotics for privacy and data protection. We contributed with a [background paper](#) on the topic (see section 4.5.4) which was very well received. Other highlights of the conference included a presentation by UN Special Rapporteur Joe Cannataci and contributions from African representatives, who underlined the importance of data protection and privacy for democracy.

The EDPS and Assistant Supervisor played an active part in the conference. EDPS Giovanni Buttarelli provided the [keynote speech](#) as part of a panel on adequacy, localisation and cultural determinism, in which he stressed the inviolable right to privacy and the need for a common framework for ethics in the digital age. The conference adopted [four resolutions](#) to which the EDPS contributed.



## The Spring Conference

The data protection authorities from the Member States of the EU and of the Council of Europe meet annually for a spring conference to discuss matters of common interest and to exchange information and experiences on different topics. The EDPS actively contributes to the discussions, which this year took place in Budapest, Hungary.

## International organisations

On 5 February 2016, the EDPS and the International Committee of the Red Cross (ICRC) hosted a workshop on data protection as part of good governance in international organisations. Taking place in Geneva, the workshop provided a forum for discussion on data protection in international organisations.

The workshop was the fifth in a series initiated by the EDPS, the first of which took place in Geneva in 2005. Our aim was to support a constructive dialogue between international organisations on data protection and privacy. As international organisations with offices in Europe are often exempt from national laws, many do not have a legal framework for data protection. This workshop was a chance to raise awareness of universal data protection principles and their consequences for international organisations. Topics of discussion included the state of play of data protection within international organisations, recent developments in data protection and privacy and the impact of these new developments on international organisations.

After the Workshop, most organisations expressed an interest in developing a more permanent forum for the discussion and exchange of information on data protection rules. We will therefore aim to hold this workshop on a more regular basis, ideally once a year.



### Case Handling Workshop

Podgorica, Montenegro hosted the 28th Case Handling Workshop, which took place in October 2016. Attended by representatives from national DPAs across Europe, the aim of the workshop was to share experiences and find ways to address the challenges we all face. The EDPS participated in the Workshop, sharing our experience of investigating complaints relating to access to data requests. The meeting is one of the few yearly events where case officers from DPAs meet to exchange ideas on data protection at the enforcement level, making it a valuable forum for discussion.

### The Berlin Group

The International Working Group on Data Protection in Telecommunications is known as the Berlin Group due to its strong support from the Berlin Commissioner for Data Protection and Information Freedom. It is made up of experts from data protection and privacy authorities, academia, civil society and global standardisation organisations, including the EDPS. Recognised as an expert group by the International Conference of Data Protection and Privacy Commissioners, the Group meets twice a year, and discusses and publishes working papers on technological developments affecting privacy. Its advice is valued not only by regulators, but also by the organisations which use these technologies.

In recent years, the Group has focused on data protection and privacy issues related to information technology, paying special attention to Internet-related developments. In 2016, the Group published a working paper on privacy and security issues in Internet Telephony and related technologies. It also continued to follow discussions on privacy issues relating to the system used to register internet domain names.

### Regional and international data protection networks

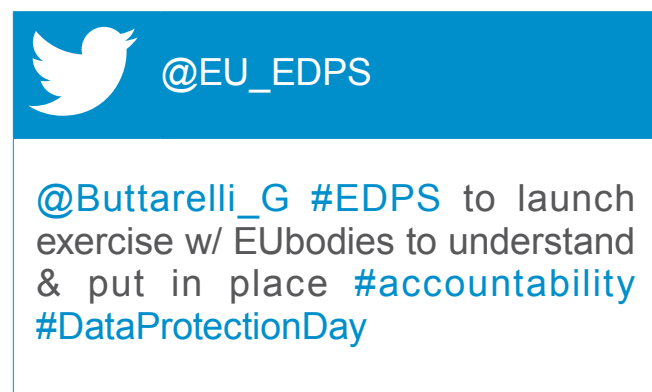
The EDPS also cooperates with regional and international networks of data protection authorities. This includes the Global Privacy Enforcement Network (GPEN), the Asia Pacific Privacy Authorities' Forum (APPA Forum), the French-speaking association of personal data protection authorities (AFAPDP), the Ibero-American data protection network (RIPD) and the International Conference of Data Protection and Privacy Commissioners (ICDPPC), including its working groups on Enforcement Cooperation and on Data Protection in Humanitarian Action.

In 2016, we participated in the exercise conducted by the WP29 and APEC to draft a common referential for EU Binding Corporate Rules (BCR) and APEC Cross-Border Privacy Rules (CBPR). We also participated in the 9th AFPDP Conference and contributed to a seminar on the impact of the new European data protection rules on Iberoamerica, organised by the RIPD. We aim to continue and extend our cooperation with regional and international networks over the coming year.

## 4.5 BEYOND COMPLIANCE

### 4.5.1 The Accountability Initiative

The new General Data Protection Regulation (GDPR) includes an explicit reference to the principle of accountability. This is the requirement for organisations themselves, rather than DPAs or DPOs, to demonstrate their compliance with data protection rules.



Accountability implies a culture change. It means promoting compliance by ensuring that the task of assessing the legality and fairness of complex data processing activities falls primarily on organisations, under the guidance of regulators, and not on the individual. Though the GDPR does not apply to the EU

institutions, the revision of the [rules that do apply to them](#) is likely to include the same emphasis on accountability.

In 2015, the EDPS launched a project to develop a framework for greater accountability in data processing. Over the course of 2016, we applied this to the EDPS, as an institution, a manager of financial resources and people, and a [controller](#), responsible for the processing of personal data. The tool we developed consists of a set of questions for the Supervisors, the Director, staff responsible for managing processing operations and our DPO. The questions do not go into specific detail, but rather aim to ensure that our organisation is in control of personal information and its lawful processing. It is hoped that the tool will serve as a useful example for other EU institutions, as they prepare for a new era in data protection.

Accountability is not new to the EU institutions. While current data protection rules do not specifically mention it, it is implicit. The EDPS, Giovanni Buttarelli, and Assistant Supervisor, Wojciech Wiewiórowski, carried out seven visits in 2016 to explain the obligations resulting from the revised legal framework, the implications for EU institutions and the role of the EDPS as their supervisory authority. The bodies visited included Frontex, the European Union Agency for Fundamental Rights (FRA), the European Court of Auditors (ECA), the European Central Bank (ECB), the Court of Justice of the European Union (CJEU), the Council of the European Union (Council) and the European Medicines Agency (EMA).

#### 4.5.2 An ethical approach to fundamental rights

The advent of the digital era has demonstrated the increasing importance of the rights to privacy and data protection. However, the exponential possibilities of digital technologies have challenged the principles of both rights and highlighted their limitations. Compliance with the law and data protection principles is important but it is also important to explore what goes beyond them.


@EU\_EDPS

[@Buttarelli\\_G](#) [#DataEthics](#) Group intends to define new ethical code in the digital environment [#CPDP2016](#)

Developing an ethical dimension to data protection is one of our [priorities for the current mandate](#). Our aim is to initiate an international debate on the ethical dimension of data protection in the digital era. Following our 2015 [Opinion](#) on digital ethics, in January 2016 we set up the [Ethics Advisory Group](#) (EAG). The group consists of six individuals, all experts in their respective fields, tasked with examining digital ethics from a variety of academic and practical perspectives.

The first EAG workshop took place in May 2016 at our offices in Brussels. Experts from the data protection community met with the members of the EAG and other experts on ethics to examine the main concerns of the data protection community. The outcome was a highly successful and insightful day of discussions, which provided valuable input for the work of the Group.

The EAG met again in October and December 2016 to discuss how ethics can contribute to a data protection regime confronted by a digital world. Their discussions emphasised the importance of not only complying with the new GDPR, but building on that compliance and the need to consider what goes beyond it.



With the balance of power between individuals and big business tipped in favour of internet giants, holding fast to our values requires more energy and commitment today than it did before the onset of the digital age. The EAG is therefore working to identify the ethical responsibilities of online actors. The greatest challenge is to encourage long term, ethical analysis and prospective thinking towards technological innovation.

The first interim report of the EAG will be published in 2017. A second EDPS-EAG workshop with experts from the scientific research community is planned for spring 2017. The conclusions of the group will provide the basis for the public session at the International Conference of Data Protection and Privacy Commissioners, which the EDPS and the Bulgarian DPA will host in 2018.

### 4.5.3 Putting the GDPR into practice

The GDPR recognises and strengthens the powers of national DPAs. This means that they will be able to advise national parliaments, governments and other institutions and bodies on legislative and administrative measures concerning the protection of personal data.

The EDPS currently enjoys similar powers. We work with the [WP29](#), made up of representatives from all EU DPAs, to ensure that our messages are consistent and to promote a single and strong EU voice on data protection matters. In 2016, we continued to invest additional resources in this area to ensure synergy with the WP29 action plan and to support their work on key elements of the GDPR. This included providing guidance for controllers and [data subjects](#) and working to interpret essential principles of the GDPR. This work will continue in 2017.

Following the adoption of the GDPR, the [data protection rules](#) applicable to the EU institutions themselves are also up for review. We expect the new rules to be in line with the GDPR and have started preparing for these changes.

One change will be the introduction of [Data Protection Impact Assessments](#) (DPIAs), which EU institutions will very likely have to carry out for particularly risky data processing operations. We have therefore started collecting information on DPIAs in other jurisdictions and have followed the work of the [WP29](#) on DPIAs at the national level, under the GDPR. In October 2016, we also [discussed DPIAs](#) at our meeting with DPOs in Alicante (see section 4.3.6). Further discussions are planned for 2017, when the proposed revision of the rules for EU institutions will be published.

### 4.5.4 Keeping track of new technology

#### IPEN: Privacy by design

The EDPS set up [IPEN](#) in 2014. This network of IT experts from academia, civil society and industry is a platform for cooperation and information exchange on better engineering methods and tools for the design and implementation of data protection and privacy requirements in systems, services and apps that use the Internet.

Throughout 2016, several conferences held panels which presented and discussed the results of work done by IPEN participants. A dedicated workshop also took place in September in Frankfurt am Main, Germany, following the [ENISA Annual Privacy Forum](#). The workshop demonstrated the increasing importance of privacy engineering following the adoption of the GDPR, which obliges anyone responsible for processing personal data to observe the principles of [data protection](#)

[by design](#) and by default. Researchers, developers and data protection regulators are increasing their efforts to strengthen and improve the technological dimension of data protection, contributing to the increasing maturity of privacy engineering as a discipline.

#### Taking back control of our online identities

The GDPR strengthens and modernises data protection rules to ensure that they are effective in the era of big data. The new rules, which include increased transparency and powerful rights of access and data portability, give users more control over their data.



On 20 October 2016, the EDPS published an [Opinion](#) on Personal Information Management Systems (PIMS). PIMS build on the developments and opportunities provided by the GDPR. They aim to strengthen fundamental rights in the digital world whilst presenting new opportunities for businesses to develop innovative personal data-based services built on mutual trust. The basic idea behind PIMS is that individuals would be able to store their personal data in secure, online storage systems and decide when and with whom to share it. PIMS offer not only a new technical architecture and organisation for data management, but also a framework for trust, providing alternative business models for collecting and processing personal data in the era of big data, and in a way that better respects European data protection law.

#### Attempting to understand artificial intelligence

Artificial intelligence (AI) is [defined as the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation](#). Much research on the topic has so far focused on machine learning, which involves the construction of algorithms that can learn from and make predictions using data. Some well-known examples include [IBM Watson](#) and [Apple Siri](#).

However, the way in which machines *learn*, through applying algorithms to data, means that, in most cases, humans cannot understand the models, or *knowledge*, produced by them. This has serious implications for data protection. If we are unable to access information about how our data is processed by these machines and, more importantly, how decisions which concern us are taken by them, it is impossible for us to meaningfully consent to the processing of our data. Getting the right information can be further complicated by organisations refusing to reveal how data is processed, on the grounds of guarding trade secrets.

As the technology develops, DPAs, including the EDPS, need to make sure that they are prepared for the changes it will bring. The importance of this was reflected at the 2016 [International Conference of Data Protection and Privacy Commissioners](#), where the closed session focused on the implications of Artificial Intelligence, machine learning and robotics for privacy and data protection. The EDPS contributed with a [background paper](#) on the topic analysing technologies such as big data and automated decision-making, image recognition, natural language processing, autonomous machines, self-driving cars and drones (see section 4.4.2).



### Unblocking the technology behind blockchain

Digital innovations, such as *virtual currencies*, have become an increasingly popular option for those seeking alternative ways of protecting their money. The privacy implications of a switch to virtual currencies, however, are yet to be determined.

The most popular virtual currency, [bitcoin](#), uses [blockchain technology](#), a kind of digital transaction ledger secured by cryptography. This blockchain is public and cannot be altered, meaning that every bitcoin transaction, including any personal data associated with the transaction, is accessible to all. As the processing of data in the blockchain is shared among all bitcoin users, it is difficult to determine who is responsible for

processing what data and how the basic principles of data protection, such as lawfulness, purpose limitation or data subject rights should be implemented.

It is essential that data protection experts begin to examine the concepts behind blockchain technology and how it is implemented in order to better understand how data protection principles can be applied to it. An integral part of this process should be the development of a privacy-friendly blockchain technology, based on the principles of privacy by design. With the aim of encouraging this approach, the EDPS participated in several events on bitcoin and blockchain in 2016, and we will continue to monitor the data protection implications of blockchain technology in the year to come.

### 4.5.5 Practical preparations for the EDPB

On 25 May 2018 the EDPB will take over the responsibilities of the WP29. The EDPB will therefore be responsible for ensuring that the GDPR is applied consistently across the EU. The EDPS will act as a member of the EDPB and provide its secretariat, although the tasks of EDPS staff providing the secretariat function will be distinct from those who represent the EDPS as a member.

EDPS staff across all units and sectors are working in close cooperation with our WP29 colleagues to ensure that the EDPB will be in place on 25 May 2018. In 2016 this included analysing options for the EDPB rules of procedure and the IT network of the Board, as well as resolving issues related to budget and service level agreements. We have kept the WP29 updated on our work by providing them with informative factsheets and reporting to them on specific actions. This includes work on IT support for the EDPB, as it is essential that we are able to provide IT systems which support the application of the GDPR, including cooperation between DPAs. Further work is planned in 2017 to ensure that the Board is fully operational by May 2018.



@EU\_EDPS

@Buttarelli\_G: #EDPS is proud to provide a modern and highly responsive secretariat to the new Data Protection Board #EDPB #data2016

#### 4.5.6 Europol: a new supervisory role for the EDPS

A new legal framework for Europol, including new data protection rules, was approved on 11 May 2016. The new Regulation assigns the EDPS responsibility for supervising the processing of personal data at Europol. It also sets up a Cooperation Board to act as an advisory body, facilitating cooperation between the EDPS and national supervisory authorities for cases relating to data from Member States. The EDPS will provide the secretariat for the Cooperation Board.

The new Regulation will apply from 1 May 2017. To prepare for this new supervisory role, we set up a dedicated internal taskforce involving all EDPS units and sectors. EDPS staff have followed internal and external training sessions related to Europol supervision and we have maintained regular contact with the DPO's Office at Europol, to foster mutual understanding and establish effective communication channels. We have also been in contact with members of the Joint Supervisory Body (JSB), which currently handles Europol supervision. We will increase our

human resources in the early part of 2017 to help manage this new responsibility.

High-level meetings between EDPS Giovanni Buttarelli and Europol Director Rob Wainwright took place in The Hague on 19 May 2016 and in Brussels on 1 December 2016. The Europol Director also gave a speech to EDPS staff, prompting useful discussions on recent developments at Europol, how to apply the [accountability](#) principle at Europol, data processing for police and justice purposes and the next steps in the transition to EDPS supervision of Europol.



## | 5. Court Cases



The EDPS can be involved in cases before the Court of Justice 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.

In 2016, we were invited to intervene in a hearing on the draft agreement between the EU and Canada on the transfer and processing of [Passenger Name Record](#) (PNR) data. We also followed closely all other cases relating to the protection of personal data. The rulings made on cases relating to data protection help us to more clearly define data protection law and to ensure that the fundamental right to privacy and data protection is fully respected.

### 5.1 EU-CANADA PNR FACES SCRUTINY

On 5 April 2016, the EDPS was invited to a [hearing](#) on the draft agreement between the EU and Canada on the transfer and processing of [PNR](#) data. The draft agreement in question was negotiated by the European Commission to replace the previous [arrangement](#), which expired in 2009. The EDPS issued an [Opinion](#) on the draft Agreement in 2013.

On 25 November 2014, the European Parliament asked the Court of Justice of the European Union (CJEU) for an opinion on the compatibility of the draft agreement

with the EU treaties and to assess whether the proposed legal basis for the agreement is appropriate.

Though the EDPS cannot intervene in such procedures on its own initiative, the CJEU can invite the EDPS, as advisor to the European institutions on data protection, to answer specific questions in writing and attend the hearing. In our [pleading](#) to the Court we made the following points:

- the draft agreement will serve as a benchmark for similar bilateral agreements with non-EU countries, which facilitate personal data transfers and have been put in place in the name of public security;
- the guarantees required under Article 8 of the [EU Charter of Fundamental Rights](#) must be respected, including when transfers are regulated in an international agreement;
- the processing of PNR data is systematic and intrusive, since it allows authorities to engage in *predictive policing*. Judicial scrutiny of EU laws on PNR must therefore be strict.

We concluded that in its present form the draft Agreement does not ensure the level of protection required under Article 8 of the Charter.

Advocate General Mengozzi published his [opinion](#) on the case on 8 September 2016. He argued that the draft agreement is partially incompatible with Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the EU, which protect the rights to privacy and data protection. The EDPS will continue to follow the case, its impact and its significance for EU data protection law in the year to come.



@EU\_EDPS

[#EDPS](#) pleading before Court of Justice - [#CanadaPNR](#)

## | 6. Transparency and Access to Documents



As an EU institution and according to its Rules of Procedure, the EDPS is subject to the Public Access to Documents Regulation of 2001. After a significant decrease in the number of public access requests received for documents held by the EDPS in 2015, the number increased again this year, rising from five requests in 2015 to 13 requests in 2016.

The EDPS will continue to respond to requests for public access to documents in 2017 and to increase the transparency of our work. This will include launching a new EDPS website, which will make it easier for users to follow the activities of the EDPS and to find the information they need.



# | 7. The Secretariat

## 7.1 INFORMATION AND COMMUNICATION

The Information and Communication team at the EDPS is responsible for ensuring that the important work done by the institution reaches its intended audience. We do this using a variety of communications tools, including online media, events, publications and press activities.

Our communications activities continued to gain momentum throughout 2016, building on the new image and approach established by the new mandate in 2015. We continue to search for effective and innovative ways to ensure that the EDPS remains at the forefront of the international debate on data protection and privacy, whether through our new website, our updated mobile app, or the EDPS blog. This momentum will continue into 2017 as we look toward the introduction of the new data protection rules and focus our attention on preparations for the EDPB.

### 7.1.1 Online media

#### Website

Throughout 2016, we continued our work on the development of a new EDPS website, which we plan to launch in early 2017. This has involved designing a new layout for the website, migrating content from the old website to the new one and transitioning to a new content management system (CMS).

The new layout is designed to be more accessible and transparent, providing easy access to EDPS work, which will be organised by topics, and to social media, through a Twitter wall. We have also introduced a powerful new search engine, making it easier for users to find the information they need.

Following the approach of the EDPS app, the website is mobile oriented and therefore easily accessible using any device.

The transition to a new CMS, EC Drupal, is also a strategic move. It will provide us with greater flexibility, both in how we present our work on the EDPS website and in the creation of additional websites in the future, such as those for the EDPB and the Supervision Coordination Groups.

The number of visitors to our current website increased significantly in 2016. This increase can be accounted for in part by our work on the transition to the new website. However, the increase is so significant that it is still safe to assume a considerable general increase in visitors to the EDPS website. This reflects the growing prominence of both the EDPS and data protection in general.



#### Social Media

Social media is an increasingly important communications tool, allowing us to easily reach a global audience. Our presence on social media is now well established. Twitter (@EU\_EDPS) remains our most influential social media tool, but we also have a strong and growing presence on both LinkedIn and YouTube.

In 2016, we witnessed another dramatic increase in followers on Twitter. Though we tweeted less than in 2015, our tweets were re-tweeted more often, in line with our aim to ensure that our tweets are both relevant and informative for those who engage with us. Our account was also officially verified by Twitter in 2016, signalling to users that it is authentic and increasing its credibility in the Twitter community.

Our presence on LinkedIn is also growing. Though the number of users who follow the EDPS has more than doubled since the end of 2015, we have been able to maintain a high average engagement rate of 1.87% with each of our posts. LinkedIn therefore remains an

excellent platform for promoting EDPS activities, events, documents and news.

In 2016, the EDPS published a record 22 videos on both YouTube and our website. The number of followers on our [YouTube channel](#) has almost doubled since the end of 2015 and the number of views of our new videos also increased in comparison to 2015. YouTube is an effective tool in helping promote our videos to a wider audience, not all of whom will have visited our website.

Our continued success on social media serves to demonstrate both our increasing global influence as an authority on data protection and our ability to reach a wider and more diverse audience.

### EDPS blog

In April 2016 we launched the [EDPS blog](#). This is a new initiative designed to provide a more detailed insight into the work of the EDPS, and of the Supervisors in particular. It is hoped that the blog will help us to reach new audiences by making data protection more accessible and understandable.

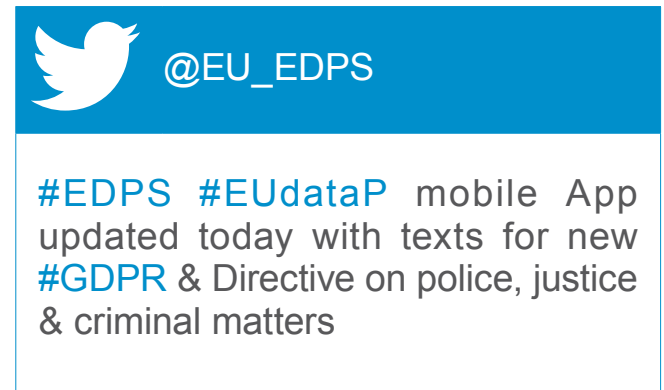
We published 16 blogposts in 2016 on a range of subjects, including the [GDPR](#), digital ethics, accountability and big data. Several of these blogposts were also distributed to our network of journalists and other interested parties. We plan to develop the blog further in 2017, giving it greater prominence as a key feature of the new website.



### EDPS mobile app

In July 2015 we released a [mobile app](#) which allowed users to compare EDPS recommendations on the GDPR with the proposed texts from the Commission, the Parliament and the Council. The app was updated in 2016 to allow users to view the final text of the GDPR alongside the initial legislative proposal of the European Commission,

the recommendations issued by the EDPS in 2015 and the rules outlined in the previous Data Protection [Directive 95/46/EC](#). It also provides a history of the reform process. Our goal was to make the legislative process more transparent and to hold the legislators to account. At the end of 2016, the app had 2205 active users.



## 7.1.2 Events and publications

### Data Protection Day 2016

On 28 January 2016, we celebrated the tenth annual Data Protection Day. We marked the occasion with several events, including a conference on the EU data protection reform for EU officials, co-hosted by the European Parliament and the EDPS, and a lunch conference on smart sharing for trainees from the EU institutions.

The annual CPDP conference, attended by data protection professionals from around the world, coincided with Data Protection Day in 2016. In addition to the various presentations given by EDPS experts at the three-day conference, we also hosted a panel on digital ethics. The event was an excellent opportunity to launch the [Ethics Advisory Group](#) (see section 4.5.2) and promote EDPS work on this topic in an international environment, in line with the goals set out in the [EDPS Strategy 2015-2019](#).

### EU Open Day 2016

On Saturday 28 May we participated in the annual Open Day of the EU institutions and bodies in Brussels. The event is an opportunity to increase general public awareness of data protection and the role of the EDPS.

As the event took place only two months after the March terrorist attacks in Brussels, security was a significant concern for both the organisers and visitors. However, despite lower visitor numbers than in past years, the EDPS stand, located in the European

Parliament, proved as popular as always. Visitors to our stand were able to interact with facial detection software and EDPS staff were on hand to answer questions. There were also promotional items available for visitors who completed our data protection quiz.

### Newsletter

The EDPS Newsletter is distributed to our Newsletter mailing list and can be found on our [website](#). We published four editions in 2016 and our mailing list continued to grow, demonstrating that the Newsletter remains an important tool for communicating our most recent and important activities.



EDPS and EU Newsroom websites and were distributed to our network of journalists and other interested parties.

In addition to this, we answered 28 written media enquiries and the EDPS and Assistant Supervisor gave 37 direct interviews to European and international journalists.

We continue to use social media alongside our press activities to enhance our media strategy and achieve maximum impact for our most influential activities. The success of this strategy helped to generate significant media coverage over the year, particularly in relation to the Privacy Shield and the GDPR. We have also seen an increase in media coverage of the EDPS in Italy and Poland, the countries of origin of the EDPS and the Assistant Supervisor respectively.

### Study visits

We hosted 12 study visit groups in 2016. These included groups from European universities and youth organisations, as well as government officials from EU countries. Through these visits, we are able to interact directly with young people and influential groups and raise awareness of the importance of data protection and the work of the EDPS.

### Information requests

The number of public information requests received by the EDPS increased significantly in 2016. The majority of these requests related to matters for which the EDPS is not competent. Others concerned requests for information on privacy matters or assistance in dealing with problems related to the protection of personal data.

The significant increase in requests received is most likely due both to the higher profile of the EDPS and to the introduction of the GDPR and the need to ensure compliance with these new rules. We replied to all requests with information relevant to the individual enquiry.

### 7.1.4 Preparations for the EDPB

#### Factsheets

In cooperation with the EDPS Human Resources, Budget and Administration (HRBA) Unit, we produced four factsheets in 2016, designed to inform members of the [WP29](#) about EDPS preparations for the new EDPB. Factsheets to date have focused on the setting up of the EDPB, human resources, budgetary and financial resources and administrative and service level agreements. More factsheets are planned for 2017.

### 7.1.3 External relations

#### Media relations

Over the course of 2016, the EDPS issued 16 press releases or statements. This represents an increase on the figures for 2015, which can be explained by the increasingly high profile of data protection and the work of the EDPS. All press releases were published on the

**Website**

The transition to a new EDPS website will serve as the starting point for the creation of the EDPB website, to be ready by May 2018. In contrast to the previous

content management system used to host the EDPS website, EC Drupal provides us with the possibility to easily create other websites based on the specifications of the new EDPS website. Work on the content and layout of the website will begin in 2017.



## 7.2 ADMINISTRATION, BUDGET AND STAFF

The Human Resources Budget and Administration (HRBA) Unit continued to provide support to the Management Board and the operational teams of the EDPS throughout 2016, to help them achieve the goals set out in the [EDPS Strategy 2015-2019](#). Our work this year included both traditional HR activities, such as a staff satisfaction survey and the EDPS staff Away Day, and new tasks, such as the setting up of the EDPB. We also developed some innovative new policies, whilst continuing to closely monitor and effectively implement our budget.

### 7.2.1 Budget and finance

#### Budget

In 2016, the EDPS was allocated a budget of EUR 9 288 043. This represents an increase of 4.55% in comparison to the 2015 budget.

Following the advice of the European Commission, we based our budget proposal for 2016 on a policy of austerity. For the fourth consecutive year, most budgetary lines remained frozen. The overall budget increase in relation to current EDPS activities was 1.3%, equalling the nominal freeze recommended by the European Commission.

Nevertheless, some additional resources were requested. These resources related to activities foreseen in the EDPS Multiannual Financial Framework 2014-2020 (MFF 2014-2020), including setting up the EDPB (see sections 4.5.5 and 7.2.2) and the new mandate for supervision of the processing activities of Europol (see section 4.5.6).

The budget implementation rate for 2016 remained high at 92%.

#### Finance

For the fifth consecutive year, the Statement of Assurance of the European Court of Auditors concerning the financial year 2015 (DAS 2015) did not raise any concerns about the reliability of our annual accounts.

However, in order to improve the efficiency of our financial management, we adopted a series of procedures:

- an updated version of the EDPS internal guide to financial transactions;

- a procedure for managing delegations for financial actors in ABAC, including new appointment forms and new charters;
- a procedure for managing the inventory of properties and fixed assets;
- accounting closure year end guidelines;
- a budgetary procedure manual.



#### Procurement

We launched two calls for tender in 2016, one on Video Production and the other on Promotional Items. The contract for Video Production was awarded in September 2016. The procedure for Promotional Items is on-going.

Some major projects and contracts were also concluded through inter-institutional Framework Contracts, including:

- **DI/07360-00(SIDE): FWC/DIGIT (EC)**
  1. Renewal of our Case Management System (CMS) VDE/SAAS and Consultancy Services
  2. Online media monitoring and international media database
- **ITS14 (Lot 2 and 3): FWC (EP)**
  1. Web Developers and Drupal Developers for the new EDPS website
  2. IT Analyst and Development Specialist for analysis and development of IT Tools

We also updated our step-by-step procedure on low value contracts and organised bilateral tutoring

sessions with the relevant members of staff to discuss the changes.

## 7.2.2 Human Resources

### The Staff Survey

In April 2016, the HR team launched a staff satisfaction survey. The questions asked were inspired by a similar survey carried out by the European Commission. The results were presented to EDPS staff and discussed in a fully transparent manner at the EDPS Away Day on 12 May 2016. Feedback from these discussions was used to develop an action plan, including concrete initiatives to improve staff satisfaction. A new survey will be launched in 2018 to follow up on our progress.

### New Policies

**Staff Retention:** In order to be successful, the EDPS relies on the talent, creativity, knowledge and commitment of its staff. As a small institution, the impact of early departures is much more costly and detrimental for the EDPS than for bigger EU institutions.

On the basis of discussions held during the EDPS Away Day on 12 May 2016, a new staff retention strategy was adopted. Existing policies have been reviewed and new actions proposed to address issues related to working conditions, recognition, motivation, communication, environment, training and career development, among others. The new strategy on staff retention will be implemented in 2017.

**Security:** In 2016 we began a review of our security policies. It is important to ensure that they remain in line with the Commission rules on security adopted in 2015, but also with the policies of other institutions, particularly Europol, which the EDPS will be responsible for supervising from 2017, and Eurojust and the European Public Prosecutor, which the EDPS could soon be responsible for supervising. The new EDPS Security Package is made up of a Decision on Security and a review of the Decision on the Protection of European Union Classified Information (EUCI), both of which we plan to finalise in 2017.

The Decision on Security concerns the general security of people, assets and information and outlines the organisational aspects of security in the EDPS. It is based on the classic principles of security, meaning respect for national law and fundamental rights and freedoms, the principles of legality, transparency, proportionality and accountability, compliance with data protection rules and the need to have a risk management assessment in place for the

implementation of security measures. The Decision also describes the tasks of all actors involved.

The reviewed Decision on the Protection of EUCI incorporates the recommendations made by the European Commission after a Security inspection carried out at the EDPS in July 2012. It ensures equivalence of protection with EU institutions on EUCI handling. Tasks related to Europol supervision are likely to result in the processing of more classified information than in the past and the amended rules provide clarity on this matter. We have also updated information on access to the so-called Secure Areas, for which we rely on the Commission.

**HRFP:** HR Forward Planning (HRFP) tools allow managers to fill the gap between current resources and future needs. Following up on a recommendation from our Internal Auditor, we developed an HRFP tool to support the Supervisors in implementing the EDPS Strategy. The EDPS HRFP has an annual cycle with several steps which help to establish the resources and HR policies needed to achieve our goals. It will therefore be a helpful tool in the development and planning of selection procedures, learning and development actions and the development and update of HR Policies or budgetary transfers.

### Accountability

**Ethics Framework:** Inspired by similar decisions at other EU institutions, we proposed the adoption of an EDPS Ethics Framework. The Framework will support the EDPS in promoting transparency, professionalism and accountability and will apply to the Supervisors, EDPS staff members, National Experts, trainees, external staff and any relations the EDPS has with the general public and external stakeholders.



The Framework encompasses administrative decisions and policies already in place, such as the Codes of Conduct for the Supervisors and for staff members, the

whistleblowing and anti-harassment Decisions, the Decision on disciplinary procedures and administrative investigations and any other future policy or decision relevant to ethical conduct. The framework foresees the appointment of an Ethics Officer to ensure internal control, raise awareness, provide advice and report to the EDPS Management Board.

**Data Protection Accountability:** The HRBA unit has been closely involved in internal discussions on the creation of an EDPS data protection accountability tool (see section 4.5.1). It is largely inspired by similar tools used by public and private organisations to ensure data protection compliance and consists of a set of questions for the Supervisors, the Director, EDPS staff who manage data processing operations and the EDPS DPO. It aims to raise awareness and obtain evidence of high-level technical and organisational measures to protect personal data and ensure accountability.

The HRBA unit provided feedback to the EDPS DPO on the questions relating to our area of activity. Once the tool was finalised in May 2016, the accountability officer set up a roadmap for answering the questions, providing evidence and creating an internal action plan for the HRBA unit. The questionnaire and the action plan demonstrate the accountability of the unit: our readiness to ensure compliance with data protection obligations and to produce documentation to prove this.

**The AGM project:** To improve the organisation of meetings and the exchange of meeting documents, the EDPS has been involved with the development of the European Commission's AGM project. In September 2016, we were designated as one of the pilot organisations.

AGM is an innovative IT application that will provide comprehensive solutions for the management of meetings of expert groups and committees, ranging from the electronic distribution of agendas and other

documents to the reimbursement of travel expenses to relevant participants. The use of this IT tool will bring substantial benefits and savings for the EDPS and the future EDPB Secretariat. It is also fully compatible with other IT systems and will automatically process a number of time-consuming tasks that would otherwise require the work of several staff members.

## EDPB

In line with the [GDPR](#), the new EDPB must be fully operational by May 2018. The EDPS, responsible for providing the EDPB Secretariat, will ensure that this new EU body receives adequate human and financial resources from the budgetary authority and that the necessary administrative set-up is in place.

We have therefore implemented an ambitious recruitment plan that includes the resources needed for the future EDPB and for the supervision of Europol, as well as some limited reinforcements for the EDPS.

**EDPB factsheets:** Providing an independent secretariat to the EDPB is a logistical and organisational challenge. This is because it is necessary to ensure confidentiality and the separation of functions whilst preserving administrative cooperation and savings for the taxpayer.

In 2016 we produced four information factsheets on the setting up of the EDPB, outlining our vision. These factsheets cover early preparations, human resources, budgetary and financial resources, and Service Level Agreements signed by the EDPS.

We trust that this information will help members of the [WP29](#) to better understand our vision and the energy we are investing in setting up the EDPB. Further details will be provided in a Memorandum of Understanding to be signed by the EDPS and the future EDPB.

## 8. The Data Protection Officer at the EDPS

### 8.1 THE DPO AT THE EDPS

The DPO at the EDPS faces the difficult tasks of meeting the expectations of colleagues, who are data protection experts, and setting the standard for the other institutions. However, he also enjoys the unique advantage of being able to benefit from his colleagues' expertise.

Even in an institution where data protection is the focus of our activities, the role of the DPO is essential to ensure effective data protection and high levels of accountability. The presence of a staff member explicitly tasked with monitoring and facilitating the protection of personal data processed within an EU institution is essential to transform a high level of awareness about data protection into action.

### 8.2 LEADING BY EXAMPLE

In 2016 we developed a tool designed to improve [accountability](#) in data protection at the EDPS (see section 4.5.1). EDPS staff from all sectors were actively involved in this exercise, coordinated and managed by the DPO. The result was a practical tool, consisting of an evidence-based questionnaire relating to all fields of data protection management.

The relevant EDPS staff members have now completed the questionnaire and the outcome of the project will be examined in detail by the DPO in 2017. The tool will be assessed and adjusted as necessary in the future, particularly to accommodate the reform of [Regulation 45/2001](#), the data protection rules which apply to the EU institutions and on which the tool is based. The initial results are positive and EDPS Giovanni Buttarelli spoke of the benefits of this experience in a series of high level accountability visits (see section 4.3.14) which took place in 2016.

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

In 2016 the DPO provided advice on a number of planned processing operations and new internal policies. These included the new EDPS website, transparency measures for the Supervisors, the EDPS Security Decision and the EDPS Information Security Policy,

Rules for Administrative Enquiries and Disciplinary Proceedings, meetings and events organised by the EDPS and the EDPS staff satisfaction survey.

### 8.4 THE REGISTER OF PROCESSING OPERATIONS

Under Article 26 of the Regulation, the DPO must keep a register of notifications for all EDPS operations involving the processing of personal data. Three new notifications were published in 2016 and several others will be completed and published in 2017.

### 8.5 PROVIDING INFORMATION AND RAISING AWARENESS

It is vitally important to raise awareness of the role of the DPO and the activities he performs amongst staff involved in processing personal data. The EDPS DPO does this in several ways.

Newcomers to the EDPS, who are not all experts in data protection, are required to attend a meeting on data protection organised by the DPO. These meetings are adapted according to the background of the staff member concerned and the role they will perform at the EDPS.

Internal EDPS coordination and information meetings, including management meetings, and the use of a dedicated Intranet page provide opportunities for the DPO to reach out to all EDPS staff. There is also a DPO section on the EDPS website, offering information about the DPO role and activities. This section is updated regularly to ensure that the DPO register and all notifications are available to the public.

The twice-yearly meetings of the DPOs of the EU institutions and bodies is a unique opportunity for the EDPS DPO to discuss common issues and share experiences and best practices with colleagues from the other EU institutions and bodies. This year, meetings took place in Dublin in April and in Alicante in October. Workshops and discussions focused on the protection of personal data in whistleblowing, research surveys, access to documents, cloud computing infrastructures, mobile devices and websites, as well as information on how to prepare for EDPS inspections and on the role of IT risk assessment in data protection (see section 4.3.6).



# 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.

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 provide 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 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](#)) and [Council framework Decision 2008/977/JHA](#) on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. These three instruments can be considered as the outcome of a legal development which started in the early 1970s in the Council of Europe.

## 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.

Directive 95/46/EC 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.

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 that has become 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 the Regulation, 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 specifically provide otherwise. The precise implications of these changes may require further clarification.

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 European 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 European level of the former Directive 97/66/EC on privacy and communications.

An interesting feature of the Regulation is the obligation for EU institutions and bodies to appoint at least one person as [data protection officer](#) (DPO). These officers have the task of 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 4.3.6).

## Tasks and powers of the EDPS

The tasks and powers of the EDPS are clearly described in Articles 41, 46 and 47 of the Regulation (see Annex B) both in general and in specific terms. Article 41 lays down the general mission of the EDPS — to ensure that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard 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 with a detailed list of duties and powers.

This presentation of responsibilities, duties and powers follows in essence the same pattern as those for national supervisory bodies: hearing and investigating complaints, conducting other inquiries, informing controllers and data subjects, carrying out prior checks when processing operations present specific risks, etc. The Regulation gives the EDPS the power to obtain access to relevant information and relevant premises, where this is necessary for inquiries. He can also impose sanctions and refer a case to the Court of Justice.

Some tasks are of a special nature. The task of advising the Commission and other institutions about new legislation — emphasised in Article 28(2) 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 have a look at privacy implications at an early stage and to discuss any possible alternatives, also 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.

The duty to cooperate with national supervisory authorities and supervisory bodies in the former *third pillar* has a similar, more strategic impact. As a member of the [Article 29 Data Protection Working Party](#), established to advise the European Commission and to develop harmonised policies, the EDPS has the opportunity to contribute at that level. Cooperation with supervisory bodies in the former *third pillar* allows him 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.

# Annex B - Extract from Regulation (EC) No 45/2001

## Article 41 — European Data Protection Supervisor

1. An independent supervisory authority is hereby established referred to as the European Data Protection Supervisor.
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 privacy, are respected by the Community institutions and bodies.

The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47.

## Article 46 — Duties

The European Data Protection Supervisor shall:

- a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;
- b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;
- c) monitor and ensure the application of the provisions of this regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;
- d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;
- e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
- f) cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body;
  - ii. also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;
- g) participate in the activities of the working party on the protection of individuals with regard to the processing of personal data set up by Article 29 of Directive 95/46/EC;
- h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);
- i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the data protection officers under Article 26;

- j) carry out a prior check of processing notified to him or her;
- k) establish his or her rules of procedure.

## Article 47 — Powers

### 1. The European Data Protection Supervisor may:

- a) give advice to data subjects in the exercise of their rights;
- b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;
- c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;
- d) warn or admonish the controller;
- e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the

notification of such actions to third parties to whom the data have been disclosed;

- f) impose a temporary or definitive ban on processing;
  - g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;
  - h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;
  - i) intervene in actions brought before the Court of Justice of the European Communities.
- ### 2. The European Data Protection Supervisor shall have the power:
- a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;
  - b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this regulation is being carried out there.

## Annex C - List of Data Protection Officers

<b>Council of the European Union</b>	<i>Carmen LOPEZ RUIZ</i>
<b>European Parliament</b>	<i>Secondo SABBIONI</i>
<b>European Commission</b>	<i>Philippe RENAUDIÈRE</i>
<b>Court of Justice of the European Union</b>	<i>Sabine HACKSPIEL</i>
<b>Court of Auditors</b>	<i>Johan VAN DAMME</i>
<b>European Economic and Social Committee (EESC)</b>	<i>Constantin CHIRA-PASCANUT</i>
<b>Committee of the Regions (CoR)</b>	<i>Michele ANTONINI</i>
<b>European Investment Bank (EIB)</b>	<i>Alberto SOUTO DE MIRANDA</i>
<b>European External Action Service (EEAS)</b>	<i>Emese SAVOIA-KELETI</i>
<b>European Ombudsman</b>	<i>Juliano FRANCO</i>
<b>European Data Protection Supervisor (EDPS)</b>	<i>Massimo ATTORESI</i>
<b>European Central Bank (ECB)</b>	<i>Barbara EGGL</i>
<b>European Anti-Fraud Office (OLAF)</b>	<i>Veselina TZANKOVA</i>
<b>Translation Centre for the Bodies of the European Union (CdT)</b>	<i>Martin GARNIER</i>
<b>European Union Intellectual Property Office (EUIPO)</b>	<i>Pedro DUARTE GUIMARÃES</i>
<b>Agency for Fundamental Rights (FRA)</b>	<i>Nikolaos FIKATAS</i>
<b>Agency for the Cooperation of Energy Regulators (ACER)</b>	<i>Marina ZUBAC</i>
<b>European Medicines Agency (EMA)</b>	<i>Alessandro SPINA</i>
<b>Community Plant Variety Office (CPVO)</b>	<i>Gerhard SCHUON</i>
<b>European Training Foundation (ETF)</b>	<i>Tiziana CICCARONE</i>
<b>European Asylum Support Office (EASO)</b>	<i>Francesca MARCON</i>
<b>European Network and Information Security Agency (ENISA)</b>	<i>Athena BOURKE</i>
<b>European Foundation for the Improvement of Living and Working Conditions (Eurofound)</b>	<i>Pierre FALLER</i>
<b>European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)</b>	<i>Ignacio VÁZQUEZ MOLINÍ</i>
<b>European Food Safety Authority (EFSA)</b>	<i>Claus REUNIS</i>
<b>European Maritime Safety Agency (EMSA)</b>	<i>Radostina NEDEVA</i>
<b>European Centre for the Development of Vocational Training (CEDEFOP)</b>	<i>Robert STOWELL</i>
<b>Education, Audiovisual and Culture Executive Agency (EACEA)</b>	<i>Dirk HOMANN</i>
<b>European Agency for Safety and Health at Work (EU-OSHA)</b>	<i>Michaela SEIFERT</i>
<b>European Fisheries Control Agency (EFCA)</b>	<i>Rieke ARNDT</i>
<b>European Union Satellite Centre (EUSC)</b>	<i>Esther MOLINERO</i>

<b>European Institute for Gender Equality (EIGE)</b>	<i>Christos GEORGIADIS</i>
<b>European GNSS Supervisory Authority (GSA)</b>	<i>Triinu VOLMER</i>
<b>European Railway Agency (ERA)</b>	<i>Zografia PYLORIDOU</i>
<b>Consumers, Health and Food Executive Agency (Chafea)</b>	<i>Despoina LEIVADINO</i>
<b>European Centre for Disease Prevention and Control (ECDC)</b>	<i>Andrea IBER</i>
<b>European Environment Agency (EEA)</b>	<i>Olivier CORNU</i>
<b>European Investment Fund (EIF)</b>	<i>Jobst NEUSS</i>
<b>European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)</b>	<i>Andrzej GRAS</i>
<b>European Securities and Markets Authority (ESMA)</b>	<i>Sophie VUARLOT-DIGNAC</i>
<b>European Aviation Safety Agency (EASA)</b>	<i>Milos PRVULOVIC</i>
<b>Executive Agency for Small and Medium-sized Enterprises (EASME)</b>	<i>Elke RIVIERE</i>
<b>Innovation and Networks Executive Agency (INEA)</b>	<i>Zsófia SZILVÁSSY</i>
<b>European Banking Authority (EBA)</b>	<i>Joseph MIFSUD</i>
<b>European Chemicals Agency (ECHA)</b>	<i>Bo BALDUYCK</i>
<b>European Research Council Executive Agency (ERCEA)</b>	<i>Joao SOARES DA SILVA</i>
<b>Research Executive Agency (REA)</b>	<i>Evangelos TSAVALOPOULOS</i>
<b>European Systemic Risk Board (ESRB)</b>	<i>Barbara EGGL</i>
<b>Fusion for Energy</b>	<i>Angela BARDENHEWER-RATING</i>
<b>SESAR Joint Undertaking</b>	<i>Laura GOMEZ</i>
<b>ECSEL</b>	<i>Anne SALAÜN</i>
<b>Clean Sky Joint Undertaking</b>	<i>Bruno MASTANTUONO</i>
<b>Innovative Medicines Initiative Joint Undertaking</b>	<i>Estefania RIBEIRO</i>
<b>Fuel Cells &amp; Hydrogen Joint Undertaking</b>	<i>Georgiana BUZNOSU</i>
<b>European Insurance and Occupations Pensions Authority (EIOPA)</b>	<i>Catherine COUCKE</i>
<b>European Police College (CEPOL)</b>	<i>Leelo KILG-THORNLEY</i>
<b>European Institute of Innovation and Technology (EIT)</b>	<i>Beata GYORI-HARTWIG</i>
<b>European Defence Agency (EDA)</b>	<i>Clarisse RIBEIRO</i>
<b>Body of European Regulators for Electronic Communications (BEREC)</b>	<i>Geoffrey DEVIN</i>
<b>European Union Institute for Security Studies (EUISS)</b>	<i>Nikolaos CHATZIMICHALAKIS</i>
<b>eu-LISA</b>	<i>Fernando DA SILVA</i>
<b>Shift2Rail Joint Undertaking</b>	<i>Sébastien PECHBERTY</i>
<b>Single Resolution Board</b>	<i>Esther BRISBOIS</i>

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

## Administration

### Anti-fraud, whistleblowing and finance

- Whistleblowing procedure, Community Plant Variety Office (CPVO), [9 November 2016](#) (2015-1065)
- Anti-fraud reporting procedure at the Education, Audiovisual and Culture Executive Agency (EACEA), [4 July 2016](#) (2013-0884)
- Fraud investigations at the European Investment Fund (EIF), [29 June 2016](#) (2014-1163)
- Whistleblowing Procedure at the European Union's Joint Undertaking for ITER and the Development of Fusion Energy (F4E), [31 March 2016](#) (2016-0087)
- Whistleblowing Procedure at the European Economic and Social Committee (EESC), [6 January 2016](#) (2015-1090)

### Administration and Human Resources

- European Commission Authentication System (ECAS) at European Banking Authority (EBA), [19 December 2016](#) (2016-1113) (Non-prior check)
- Administrative inquiries and disciplinary proceedings, European Maritime Safety Agency (EMSA), [19 December 2016](#) (2014-0287)
- Administrative inquiries and disciplinary proceedings, European Investment Fund (EIF), [14 December 2016](#) (2015-1103)
- Staff absences, European Institute for Gender Equality (EIGE), [11 November 2016](#) (2013-0789)
- Online coaching for interpreters, European Parliament, [10 October 2016](#) (2015-1125)
- Management of incident reports, Court of Justice of the European Union (CJEU), [12 September 2016](#) (2013-0786)

- Management of traineeships at the European Economic and Social Committee (EESC) - Update, [7 September 2016](#) (2005-0297 and 2009-0701)
- Administrative inquiries and disciplinary proceedings at the Community Plant Variety Office (CPVO) - Update, [20 July 2016](#) (2011-1128)
- Administrative inquiries and disciplinary procedures at the European Insurance and Occupational Pensions Authority (EIPOA), [17 June 2016](#) (2016-0415)
- Administrative inquiries and disciplinary proceedings at the European Global Navigation Satellite Systems Agency (GSA), [14 June 2016](#) (2016-0262)
- Processing of health data at the European Securities and Markets Authority (ESMA), [18 May 2016](#) (2013-0927)
- Access to the professional/personal data of staff members in the event of absence, departure from EIF service or death, European Investment Fund (EIF), [18 May 2016](#) (2015-0808) (Non-prior check)
- Access to the professional/personal data of staff members in the event of absence, leaving the Bank or death, European Investment Bank (EIB), [18 May 2016](#) (2013-0801) (Non-prior check)
- Processing of health data at the European Union Agency for Network and Information Security (ENISA), [31 March 2016](#) (2011-1149)
- Processing of health data at the European Global Navigation Satellite Systems Agency (GSA), [17 March 2016](#) (2015-1129)
- Internal mobility at the European Aviation Safety Agency (EASA), [10 March 2016](#) (2013-1354)
- Processing of health data at Electronic Components and Systems for European Leadership joint undertaking (ECSEL), [1 March 2016](#) (2013-0956)

- Processing of health data at the European Banking Authority (EBA), [26 February 2016](#) (2013-1065)
- Processing of health data and administrative data related to health at the European Defence Agency (EDA), [16 February 2016](#) (2013-0740)
- Management of health data at SESAR Joint Undertaking, [16 February 2016](#) (2013-0839)
- Management of health data at CLEAN SKY Joint Undertaking, [16 February 2016](#) (2013-0934)
- Management of health data at Innovative Medicines Initiative (IMI), [16 February 2016](#) (2013-0616)
- Use of thermal imaging cameras and the auto-track functionality of pan-tilt cameras at the European Central Bank (ECB), [1 February 2016](#) (2015-0938)
- Video-surveillance at BEREC, 8 January 2016 (2015-1089) (Non-prior check)
- Individual performance indicators for the annual evaluation of staff members at the Community Plant Variety Office (CPVO), [4 July 2016](#) (2016-0417)
- Staff reclassification exercise at eu-LISA, [2 June 2016](#) (2015-0916)
- Staff evaluation procedures at the European Securities and Market Authority (ESMA), [10 May 2016](#) (2013-0928)
- Probation procedures at the European Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), [10 May 2016](#) (2015-0908)
- Staff performance appraisal at the European Investment Fund (EIF), [31 March 2016](#) (2014-1141)

#### Anti-harassment

- Anti-harassment procedures at the European Network and Information Security Agency (ENISA), [25 July 2016](#) (2013-0920)
- Selection of confidential counsellors at the European Institute for Gender Equality (EIGE), [20 July 2016](#) (2016-0408)
- Selection of confidential counsellors and of the informal procedure for cases of alleged harassment at the European Global Navigation Satellite Systems Agency (GSA), [14 June 2016](#) (2016-0263)
- Confidential staff counselling of the European Centre for Disease Prevention and Control (ECDC), [22 April 2016](#) (2013-0790)
- Selection of confidential counsellors and of the informal procedure for cases of alleged harassment at the European Securities and Markets Authority (ESMA), [22 January 2016](#) (2015-1040)

#### Evaluation (360° and Staff Appraisal)

- Assessment of statutory staff's skills and competencies at the European Union Agency for Railways, [5 August 2016](#) (2016-0538)
- 360° Multi-source feedback exercise tool at the European Central Bank (ECB), [27 July 2016](#) (2015-0772)

#### Grants and Public Procurement

- Independent expert management in the context of Horizon 2020 at DG RTD, European Commission, [14 November 2016](#) (2016-0950)
- Grant management in the context of Horizon 2020 at DG RTD, European Commission, [14 November 2016](#) (2016-0951)
- Public procurement at the European Institute of Innovation and Technology (EIT), [2 June 2016](#) (2015-0516)

#### Recruitment

- Selection, Recruitment and Administrative Management for Seconded National Experts in EEAS Headquarters and EU Delegations, European External Action Service (EEAS), [9 December 2016](#) (2016-0769)
- Selection procedures for Seconded National Experts (SNE), European Network and Information Security Agency (ENISA), [23 November 2016](#) (2010-0935)
- E-recruitment at the Community Plant Variety Office (CPVO), [25 July 2016](#) (2016-0492)
- Selection and recruitment of staff at the European Investment Fund (EIF), [4 March 2016](#) (joint cases 2014-0861, 2014-1065 and 2014-1067)
- Appointment procedures of Chairs and Executive Directors of the European Supervisory Authorities, European Parliament, [14 January 2016](#) (2015-1028)



- Selection, recruitment and management of bluebook trainees, Research Executive Agency (REA), [12 January 2016](#) (2015-0760)

## Core Business

- Import, Export and Transit Directory, European Anti-Fraud Office (OLAF), [7 December 2016](#) (2016-0674 and 2013-1296)
- PeDRA - Personal data in Risk Analysis, European Border and Coast Guard Agency (Frontex) - Update, [24 November 2016](#) (2015-0346)
- European Aero-Medical Repository (EAMR) project at European Aviation Safety Agency (EASA), [19 July 2016](#) (2016-0271) (Non-prior check)
- Creation of insider lists for the prevention of insider dealing and market manipulation at the European Investment Bank (EIB), [29 June 2016](#) (2016-0497) (Non-prior check)
- Activities of the Equal Opportunities Office at the General Secretariat of the Council of the European Union, [17 June 2016](#) (2016-0123)
- EU Platform for Rare Diseases Registration at the Joint Research Centre-Ispra (JRC), [17 June 2016](#) (2015-0982)
- Antifraud Transit Information System (ATIS) at the European Anti-Fraud Office (OLAF), [18 May 2016](#) (2013-1296)

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

## Opinions

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

In 2016 the EDPS issued Opinions on the following subjects (date of publication in brackets):

- Personal Information Management Systems (20 October 2016)
- Coherent enforcement of fundamental rights in the age of Big Data (23 September 2016)
- The First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations) (21 September 2016)
- The Second EU Smart Borders Package (21 September 2016)
- ePrivacy (22 July 2016)
- The EU-US Privacy Shield draft adequacy decision (30 May 2016)
- The exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS) (13 April 2016)
- European Border and Coastal Guard Regulation (18 March 2016)
- EU-US umbrella agreement (12 February 2016)

## Formal comments

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

In 2016 the EDPS issued formal comments on the following subjects (date of publication in brackets):

- Commission Implementing Regulation laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment (14 December 2016)
- Proposal amending Directive 98/41 on registration of persons on board passenger ships (9 December 2016)

# Annex F - Speeches by the Supervisor and Assistant Supervisor in 2016

## European Parliament

Supervisor, LIBE Hearing on The Reform of the Dublin System and Crisis Relocation, speech given by Giovanni Buttarelli Parliament, Brussels (10 October 2016)

Supervisor, [LIBE Data protection: High-level hearing on the new EU-US “Privacy Shield” for commercial transfers of EU personal data to the US](#), replacing the former “Safe Harbour”, speech by Giovanni Buttarelli, European Parliament, Brussels (17 March 2016)

Supervisor, [Preliminary opinion on the EU-US “Umbrella Agreement”](#), given by Giovanni Buttarelli at Civil Liberties, Justice and Home Affairs Committee (LIBE), Brussels (15 February 2016)

## Other EU Institutions and bodies

Assistant Supervisor, *Big Data Means Big Responsibility. Privacy in the algorithmic world*, lecture at the debate EU Big Data Regulation, organised by the College of Europe, Brussels (12 December 2016)

Supervisor, [The accountability principle in the new GDPR](#), European Court of Justice, Luxembourg (30 September 2016)

Supervisor, [Convention 108: from a European reality to a global treaty](#), Council of Europe International Conference, Strasbourg, France (17 June 2016)

Assistant Supervisor, *Why does data protection matter?*, lecture at the seminar *Smart Sharing*, organised by the EDPS, Brussels (28 January 2016)

## International Conferences

Supervisor, [The 7th Annual European Data Protection and Privacy Conference](#), Brussels (1 December 2016)

Assistant Supervisor, *International Cooperation, Personal Data Protection Agreements, Relevant*

*experiences, Convention 108*, lecture during 46th APPA Forum, Manzanillo, Mexico (30 November-2 December 2016)

Supervisor, [Encryption protects security and privacy](#), given at the conference *Chiffrement, Sécurité et Libertés* at Assemblée nationale française, Paris, France (21 November 2016)

Supervisor, [IAPP Europe Data Protection Congress 2016](#), keynote speech by Giovanni Buttarelli, Brussels (9 November 2016)

Supervisor, [Privacy in an age of hyperconnectivity](#), keynote speech to the Privacy and Security Conference 2016, Rust am Neusiedler See, Austria (7 November 2016)

Assistant Supervisor, *New Legal Framework for data Protection Law in the European Union*, lecture at the 7th international Personal Data Protection Conference, Moscow, Russia (7-8 November 2016)

Supervisor, [Les données personnelles: entre protection et exploitation](#), at the Autumn School 2016 on the EU, University of Laval, Québec, Canada (4 November 2016)

Assistant Supervisor, *The Rule of Law in the Technological Age - the Impact of New Technologies on Privacy and Data Protection*, lecture during 6th ACELG's Annual Conference 2016, Amsterdam, Netherlands (4 November 2016)

Supervisor, *New instruments to promote the correct application of the EU charter of fundamental rights at the national level*, Rome, Italy (28 October 2016)

Supervisor, [Adequacy, Localisation and Cultural Determinism](#), 38th International Privacy Conference, Marrakech, Morocco (19 October 2016)

Supervisor, [SC Intelligence on Science Seminar - “The Impact of the General Data Protection Regulation on collaborative science in Europe and the European Cloud Initiative”](#), (video), Brussels (18 October 2016)

Supervisor, [Belgian Senate Conference - Issues of citizens' privacy and data protection in relation to new technologies](#), (video), Brussels (17 October 2016)

Assistant Supervisor, *In cooperation we (will) trust*, lecture at II Workshop of PHAEDRA II at the 38th International Privacy Conference, Marrakesh, Morocco (16-21 October 2016)

Assistant Supervisor, *EU GDPR: What do Cloud providers need to know for 2018?*, lecture at EuroCloud Forum 2016, Bucharest, Romania (5-6 October 2016)

Assistant Supervisor, *Reporting Data Breaches* (video), lecture at Security Case Study 2016, Warsaw, Poland (September 14-15 2016)

Supervisor, SEC2SV - European Innovation Day, (12 September 2016)

Assistant Supervisor, *Developing and Maintaining a Privacy Enhancing Technology Maturity Repository*, lecture at the *ENISA Annual Privacy Forum 2016, Bringing Research & Policy Together*, Frankfurt, Germany (7-8 September 2016)

Supervisor, CISO Coalition webinar, videoconference (2 August 2016)

Supervisor, 45th APPA forum, Singapore (19 July 2016)

Supervisor, [Global Personal Data Protection Policy Trend](#), keynote speech by Giovanni Buttarelli given at Korea Internet and Security Agency (KISA), Seoul, South Korea (video message) (18 July 2016)

Assistant Supervisor, *How data protection rules should be enforced in tandem with competition and consumer policy*, lecture at the 29th Annual Conference of Privacy Laws & Business, *Great Expectations*, Cambridge, United Kingdom (4-6 July 2016)

Assistant Supervisor, *Empowering rights holders*, speech at the *Fundamental Rights Forum 2016*, Vienna, Austria (20-23 June 2016)

Supervisor, *Connected Citizens Summit*, Amsterdam, The Netherlands (21 June 2016)

Supervisor, BEUC Digiforum 2016: [Consumers shaping the digital economy](#), Brussels (20 June 2016)

Assistant Supervisor, *Data protection and new telecoms. What are the privacy challenges for new devices?*, speech at the 27th Annual IBA

Communications and Competition Conference, Amsterdam, The Netherlands (6-7 June 2016)

Supervisor, [Spring Conference of European DPAs](#), Budapest, Hungary (26 May 2016)

Assistant Supervisor, *The role of guidelines, recommendations and codes of best practices in encouraging consistent application of GDPR*, lecture at the Spring Conference of European Data Protection Authorities, Budapest, Hungary (25-27 May 2016)

Assistant Supervisor, *Data Protection, Privacy and National Security*, lecture at the *Cyber Conference 2016*, London, United Kingdom (23-24 May 2016)

Supervisor, [Key Challenges for Privacy in the Digital Age](#), Europol/EIPA conference on Privacy in the Digital Age of Encryption and Anonymity Online, The Hague, The Netherlands, (19 May 2016)

Supervisor, 6th EUROFORUM-Conference "European Data Protection Days", Berlin, Germany (25 April 2016)

Assistant Supervisor, *How does the emergence of online platforms affect the Digital Single Market?*, lecture at the 10th Digital Regulation Forum, *Policies for the Digital Single Market. An Evolution or a Revolution*, London, United Kingdom (20-21 April 2016)

Supervisor, [Counterterrorism and Data Privacy: A European Perspective](#), to the symposium on Governing Intelligence: Transnational Approaches to Oversight and Security, hosted by the Center on Law and Security and the Woodrow Wilson International Center for Scholars, New York, United States (21 April 2016)

Supervisor, [Ethics at the Root of Privacy and as the Future of Data Protection](#), event hosted by Berkman Center for Internet and Society at Harvard University and the MIT Internet Policy Initiative and the MIT Media Lab, Boston, United States (19 April 2016)

Supervisor, IAPP Conference, Washington D.C., United States (4 April 2016)

Supervisor, [Living in a future Big Data world: can prosperity, freedom and fundamental rights be reconciled?](#), Keynote address by Giovanni Buttarelli to the Delphi Economic Forum, Delphi, Greece (27 February 2016)

Supervisor, [Speech to a conference on personal data protection in churches and religious organisation](#) given by Giovanni Buttarelli at Opole University and the

University of Szczecin, Warsaw, Poland (25 February 2016)

Supervisor, [Opening address at the Fifth Workshop on Data Protection in International Organisations](#), Geneva, Switzerland (5 February 2016)

Supervisor, [Closing remarks](#) by Giovanni Buttarelli given at the 9th International Computers, Privacy and Data Protection Conference, Brussels (29 January 2016)

Assistant Supervisor, *Making the Regulation Work In Practice, speech* at the 9th CPDP Conference, Brussels (27-29 January 2016)

## Other events

Supervisor, *Il nuovo regolamento privacy e la sua applicazione nel settore pubblico e privato*, Rome, Italy (16 December 2016)

Supervisor, *Conference on Economic Developments in European Competition Policy, Big Data and the Search for a Competition Problem*, Brussels (7 December 2016)

Supervisor, *ICT4intel 2020 - Edizione 2016*, Rome, Italy (18 November 2016)

Supervisor, [Coalition for Cybersecurity and Law Symposium Cybersecurity under the next president: A Symposium with cybersecurity industry leaders](#), closing speech by Giovanni Buttarelli, San Francisco, United States (15 November 2016)

Assistant Supervisor, *Algorithmic Transparency at the Age of Artificial Intelligence (video from 5'15")*, lecture at the IEEE AI & Ethics Summit 2016, Brussels (15 November 2016)

Assistant Supervisor, *Case Study: Connected Cars, No Longer Emerging but Reality* at the European Data Protection Congress, Brussels (9-10 November 2016)

Assistant Supervisor, *Privacy and Genomic Data: What Are the Real Risks?*, at the European Data Protection Congress, Brussels (9-10 November 2016)

Assistant Supervisor, *Reform of the EU Data Protection Law* (Unijna reforma ochrony danych osobowych), lecture at the conference Human Being in the Cyberspace (Człowiek w cyberprzestrzeni), Warsaw, Poland (11 October 2016)

Supervisor, *Data Protection in the era of Big Data - a look at financial services, insurance and healthcare*, Luxembourg (30 September 2016)

Supervisor, [Big Data individual rights and enforcement](#), speech at EDPS-BEUC Joint Conference, Brussels (29 September 2016)

Supervisor, *Privacy e protezione dei dati personali: il regolamento UE 2016/679*, Bologna, Italy (26 September 2016)

Supervisor, [Europe's big data protection opportunity](#), keynote address of Giovanni Buttarelli given at the Banking and Payments Federation, London, United Kingdom (15 September 2016), video conference

Supervisor, *Data Protection Whitepaper*, Brussels (14 July 2016)

Assistant Supervisor, *Role of the Data Protection Officer in IT Accountability* (Rola Administratora Bezpieczeństwa Informacji w zapewnieniu rozliczalności w zakresie IT) ([video](#)), lecture at the conference Data Protection Officer, Warsaw, Poland (29 June)

Supervisor, *International Conference European Digital Day, What impact of the data protection on the future of a global digital economy?*, Paris, France (17 June 2016)

Assistant Supervisor, *Why Will We Love Internet of Things and Why Should We Be Careful Being in Love ?- IoT: A Sustainable Way Forward*, at EuroDIG 2016, Brussels (9-10 June)

Assistant Supervisor, *Large Scale Resources of Health Related Data in the Light of Data Protection Law* (Przetwarzanie dużych zasobów danych o zdrowiu w świetle prawa ochrony danych osobowych) ([video](#)), lecture at the conference Biobanks – Challenges of Big Data, Warsaw, Poland (8 June 2016)

Assistant Supervisor, *Four Pillars for the Acceptable Interference in the Right to Privacy in Cybersecurity* (Cztery filary dopuszczalnej ingerencji w prawo do prywatności w ramach działań 'cyberobronnych'), lecture at 8th Conference Internet Security - Cybersecurity Strategy for Poland. Institutional and Legal Aspects, Warsaw, Poland (19-20 May 2016)

Supervisor, *IV Congreso Nacional de Privacidad APEP*, (video message) Barcelona, Spain (19 May 2016),

Assistant Supervisor, *Public Security Motivated Surveillance. Four Pillars for the Acceptable*

*Interference in the Right to Privacy*, lecture at the conference *Surveillance, How Far You Can Go?*, Warsaw, Poland (14 May 2016)

Supervisor, British Chamber of Commerce in Denmark: event on EU Data Protection Reforms: Privacy Shield: Opportunities out of New Rules, Copenhagen, Denmark (10 May 2016)

Supervisor, *European Union as a promoter of a real revolution*, article of Giovanni Buttarelli in *Il Sole 24 Ore* newspaper (9 May 2016)

Assistant Supervisor, *Regulation: Herald of Positive Change*, panelist at *Privacy: The Competitive Advantage*, London, United Kingdom (29 April 2016)

Assistant Supervisor, *Privacy Protection on the Web. The Role of User, Market and Public Authorities* (*Ochrona prywatności w Sieci. Rola użytkownika, rynku i podmiotów publicznych*), lecture at the University of Białystok, Białystok, Poland (8 April 2016)

Assistant Supervisor, *Protection of Personal Data in the Digital Single Market* (*Ochrona danych osobowych na jednolitym rynku cyfrowym*), lecture at the conference *Electronic Media Forum. Digital Europe* (*Forum Mediów Elektronicznych. Europa Cyfrowa*), Opole, Poland (6-7 April 2016)

Supervisor, *Seminario Privacy Shield* (22 March 2016)

Supervisor, [Les données et la concurrence dans l'économie numérique](#), Opening statement at the Roundtable on data and competition hosted by l'Autorité de la Concurrence, Paris, France (8 March 2016)

Assistant Supervisor, *Personal Data in the IoT Driven Smart City* (*Dane osobowe w inteligentnym mieście korzystającym z rozwiązań Internetu rzeczy*), lecture at the 9th New Economy Forum, Smart Cities in Transformation, Krakow, Poland (25 January 2016).

# | Annex G - Composition of EDPS Secretariat



## Director, Head of Secretariat

Christopher DOCKSEY

Christian D'CUNHA  
*Policy Assistant to the EDPS*

Hielke HIJMANS \*  
*Special Adviser*

Daniela OTTAVI \*  
*Planning/Internal Control Coordinator*

## Supervision and Enforcement

Maria Verónica PEREZ ASINARI  
*Head of Unit*

Isabelle Chatelier  
*Head of Complaints and Litigation*

Bénédicte RAEVENS  
*Acting Head of Prior Checks and Consultation*

Ute KALLENBERGER  
*Head of Inspections*

Stephen ANDREWS  
*Supervision and Enforcement Assistant*

Petra CANDELLIER  
*Legal Officer*

Claire GAYREL  
*Legal Officer*

Mario GUGLIELMETTI  
*Legal Officer*

Delphine HAROU  
*Legal Officer*

Xanthi KAPSOSIDERI  
*Legal Officer*

Owe LANGFELDT  
*Legal Officer*

Anna LARSSON STATTIN  
*Legal Officer/Seconded National Expert*

Snezana SRDIC  
*Legal Officer*

Tereza STRUNCOVA  
*Legal Officer*

## Policy and Consultation

Sophie LOUVEAUX  
*Head of Unit*

Anne-Christine LACOSTE  
*Head of International Cooperation*

Anna BUCHTA  
*Head of Litigation and Institutional Policy*

Zsuzsanna BELENYESSY  
*Legal Officer*

Gabriel Cristian BLAJ \*  
*Legal Officer*

Katinka BOJNAR  
*Legal Officer/Seconded National Expert*

Alba BOSCH MOLINE  
*Legal Officer*

Priscilla DE LOCHT  
*Legal Officer*

Anna COLAPS \*  
*Policy and Consultation Assistant*

Amanda JOYCE  
*Policy and Consultation Assistant*

Zoi KARDASIADOU  
*Legal Officer/Seconded National Expert*

Jacob KORNBECK  
*Legal Officer*

Fabienne MOLLET  
*Administrative Assistant*

Fabio POLVERINO  
*Legal Officer*

Romain ROBERT  
*Legal Officer*

Lara SMIT  
*Legal Officer*

Evelien VAN BEEK \*  
*Legal Officer*

Gabriela ZANFIR \*  
*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*

Malgorzata LAKSANDER  
*Technology and Security Officer*

Fredrik LINDHOLM  
*Administrative Assistant*

Fidel SANTIAGO  
*Technology and Security Officer*

## Records Management

Luisa PALLA  
*Head of Sector*

Marta CÓRDOBA HERNÁNDEZ  
*Administrative Assistant*

Denisa IONICA  
*Administrative Assistant*

Kim Thien LÊ  
*Administrative Assistant*

Séverine NUYTEN  
*Administrative Assistant*



Maria José SALAS MORENO  
*Administrative Assistant*

Sonya SOMRANI PEREZ  
*Administrative Assistant*

Martine VERMAUT  
*Administrative Assistant*

## Information and Communication

Olivier ROSSIGNOL  
*Head of Sector*

Francesco ALBINATI  
*Information and Communication Officer*

Thomas HUBERT  
*Web Developer/Graphic Designer*

Courtenay MITCHELL  
*Information and Communication Officer*

Parminder MUDHAR  
*Information and Communication Officer*

Agnieszka NYKA  
*Information and Communication Officer*

Benoît PIRONET  
*Web Developer*

## Human Resources, Budget and Administration

Leonardo CERVERA NAVAS  
*Head of Unit*

Sylvie PICARD  
*Head of Human Resources Coordination and Planning*

Marian SANCHEZ LOPEZ  
*Head of Finance*

Cláudia BEATO  
*Human Resources Assistant*

Pascale BEECKMANS  
*Human Resources Assistant  
GEMI*

Laetitia BOUAZZA-ALVAREZ  
*Human Resources Assistant  
GECO  
Traineeship Coordinator*

Vittorio MASTROJENI \*  
*Human Resources Officer*

Julia MOLERO MALDONADO  
*Finance Assistant*

Marco MORESCHINI  
*Human Resources Officer/Seconded National Expert  
LSO*

Carolina POZO LOPEZ  
*Administrative Assistant*

Karina REMPESZ  
*Human Resources Officer  
L&D Coordinator*

Anne-Françoise REYNDERS  
*Human Resources Officer*

Caroline WOUSSEN-DUBUISSEZ  
*Finance Assistant*

\*staff members who left the EDPS in the course of 2016

## HOW TO OBTAIN EU PUBLICATIONS

### Free publications:

- one copy:  
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:  
from the European Union's representations ([http://ec.europa.eu/represent\\_en.htm](http://ec.europa.eu/represent_en.htm));  
from the delegations in non-EU countries ([http://eeas.europa.eu/delegations/index\\_en.htm](http://eeas.europa.eu/delegations/index_en.htm));  
by contacting the Europe Direct service ([http://europa.eu/europedirect/index\\_en.htm](http://europa.eu/europedirect/index_en.htm)) or  
calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (\*).

(\*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

### Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

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

