EDPS

European Data Protection Supervisor

Annual **Report**

2017

An Executive Summary of this report, which gives an overview of key developments in EDPS activities in 2017, 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.

The image on the cover represents a database. Each of the four parts relates to EDPS work, the world of data and data protection in general:

- Security and protection, represented by data cells and padlocks.
- The relationship between people and the digital world, represented by the individual
- The global nature of data protection, the exchange of data and our connection with the digital world
- Data in general, represented by binary code, the numerical translation of all things related to data.

Luxembourg: Publications Office of the European Union, 2018

PDF	ISBN 978-92-9242-130-4	ISSN 1830-9585	doi:10.2804/084169	QT-AA-18-001-EN-N
Print	ISBN 978-92-9242-131-1	ISSN 1830-5474	doi:10.2804/07566	QT-AA-18-001-EN-C
EPUB	ISBN 978-92-9242-129-8	ISSN 1830-9585	doi:10.2804/72879	QT-AA-18-001-EN-E

Annual **Report**

2017

European Data Protection Supervisor

Contents

TABLES AND GRAPHS

Foreword

We are now only a few short months away from a historic moment for EU data protection. The new General Data Protection Regulation (GDPR) will apply from 25 May 2018, ushering in a new era of data protection designed for the digital age.

The GDPR is an outstanding achievement for the EU, its legislators and stakeholders, but the EU's work to ensure that data protection goes digital is far from finished.

2017 marked the first year in which the majority of the world's population reported having access to the internet. Tech giants now represent the six highest valued companies in the world and, with their immense market and informational power, they are capable of reaching into the most intimate aspects of our private lives.

Simultaneously, the constant tracking we are subjected to online is eliciting a backlash, evident in the growth in the use of VPNs, encryption and ad blockers, as well as the controversy over the micro targeting of individuals with manipulative fake news.

With this in mind, it is more important than ever that the EU develop appropriate legislation on ePrivacy to complement the GDPR and ensure that electronic communication between individuals remains secure and confidential.

Addressing the risks associated with monopoly power in digital markets, premised on constant covert tracking, requires more than this, however. Part of the solution is closer cooperation between regulators; but a genuine cultural sensitivity to the ethical dimension of decision-making is also indispensable.

With individuals increasingly subjected to varying methods of surveillance, people are beginning to talk about developing a digital ethics, and the EDPS

intends to be a leading force in this area. Through the international conference we will host in October 2018, we hope to inspire much-needed debate on this topic across the world and across disciplines, as well as to prepare independent data protection authorities (DPAs) to act as respected guides on the responsible development and application of Artificial Intelligence.

The concerns raised in the debate on digital ethics must also inform current debates on the value of personal data, including the concept of paying with personal data, referenced in the proposed Digital Content Directive. At the request of the Council, we were able to influence the debate on this proposal through the publication of our March 2017 Opinion, and we hope to remain a trusted and influential partner on similar issues in the years to come.

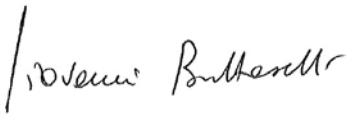
Finalising and implementing a revised version of the current legislation governing data protection in the EU institutions and bodies as soon as possible is also essential, if the EU is to remain a credible and effective leader in the protection of individuals' rights.

At the EDPS, we intend to exercise the powers that will be granted to us in the revised Regulation efficiently and responsibly, in an effort to ensure that the EU's institutions and bodies set an example for the rest of the EU to follow. We have invested a lot of effort in preparing our fellow institutions for the new rules, raising awareness of new principles such as accountability at the highest level and training staff for the switch from prior checking processing operations to Data Protection Impact Assessments (DPIAs).

Meanwhile, the EU is coming of age as a responsible facilitator of the exchange of personal data between police forces around the continent. The legal basis for Europol was renewed for the post-Lisbon Treaty era to include a set of standards for personal data processing designed to deal with the challenges of the future.

We have adjusted swiftly to our new responsibilities at Europol and are committed to ensuring that the agency sets an example, by striking the right balance between security and privacy when dealing with data processing for the purpose of law enforcement.

With 25 May 2018 drawing ever closer, preparations for the launch of the European Data Protection Board (EDPB) are now well underway. Supported by a high quality secretariat, the Board will take over the responsibilities currently assumed by the Article 29 Working Party (WP29), as well as performing other tasks to ensure the consistent application of the GDPR across the EU. As we move forward into a new era in data protection and privacy practice, the EDPS will continue our efforts to lead by example in the global dialogue on data protection and privacy in the digital age.



Giovanni Buttarelli
European Data Protection Supervisor

Wojciech Wiewiórowski
Assistant Supervisor

Mission statement, values and principles

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

In order to protect and guarantee the rights to data protection and privacy, the processing of personal data is subject to control by an independent authority. 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 policy making, legislating and judicial entity looks to the EDPS as an independent supervisor and impartial advisor on policies and proposed laws which might affect the rights to privacy and data protection. The EDPS performs these functions by establishing itself as a centre of excellence in the law, and also in technology, insofar as it affects or is affected by the processing of personal data.

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

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

Core values

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

Guiding principles

- We serve the public interest to ensure that EU institutions comply with data protection principles in practice. We contribute to wider policy as far as it affects European data protection.
- Using our expertise, authority and formal powers, we aim to build awareness of data protection as a fundamental right and as a vital part of good public policy and administration for EU institutions.
- We focus our attention and efforts on areas of policy or administration that present the highest risk of non-compliance or the greatest impact on privacy. We act selectively and proportionately.

EDPS Strategy 2015-2019

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

About the Strategy

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

The 2015-2019 strategic plan summarises:

- the major data protection and privacy challenges over the 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 Actions 2015-2019

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

1 Data protection goes digital

(1) promoting technologies to enhance privacy and data protection;

(2) identifying cross-disciplinary policy solutions;

(3) increasing transparency, user control and accountability in big data processing.

2 Forging global partnerships

(4) developing an ethical dimension to data protection;

(5) speaking with a single EU voice in the international arena;

(6) mainstreaming data protection into international policies.

3 Opening a new chapter for EU data protection

(7) adopting and implementing up-to-date data protection rules;

(8) increasing accountability of EU bodies collecting, using and storing personal information;

(9) facilitating responsible and informed policymaking;

(10) promoting a mature conversation on security and privacy.

@EU_EDPS

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

1. About the EDPS

The EDPS ensures that the European institutions and bodies respect the fundamental rights to privacy and data protection, whether they are involved in processing personal data or in developing new policies. We have three main fields of work:

- **Supervision:** We monitor the processing of personal data by the EU administration and ensure that they comply with data protection rules. Our tasks range from prior checking processing operations likely to present specific risks, to handling complaints and conducting inquiries.
- **Consultation:** We advise the European Commission, the European Parliament and the Council on proposals for new legislation and other issues related to data protection.
- **Cooperation:** We work with national data protection authorities (DPAs) to promote consistent data protection across the EU. Our main platform for cooperation with DPAs is the Article 29 Working Party (WP29).

The EU institutions must comply with the data protection rules set out in Regulation 45/2001, which the EDPS is required to enforce. 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), which was finalised at the end of 2015. Regulation 45/2001, which outlines the roles and responsibilities of the EDPS, is currently under revision to bring it in line with the GDPR.

With this in mind, the EDPS is not only focused on ensuring compliance with current legislation but with anticipating and preparing for the changes to come, as is reflected in our Strategy 2015-2019.

1.1 SUPERVISION AND ENFORCEMENT

The EDPS aims to ensure that EU institutions are not only aware of their data protection obligations, but can also be held accountable for complying with them. We have several tools we can use, all of which are aimed at encouraging the development of a data protection culture in the EU institutions:

- **Prior checks:** EU institutions and bodies must inform the EDPS of any procedures they plan to carry out which might pose a risk to the protection of personal data. The EDPS examines the proposals and provides recommendations on how to address these risks.
- **Complaints:** We handle complaints from individuals relating to the processing of personal data by the EU institutions. We investigate these complaints and decide on the best way to handle them.
- **Monitoring compliance:** The EDPS is responsible for ensuring that all EU institutions and bodies comply with 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.
- **Guidance:** We issue Guidelines for the EU institutions, designed to help them better implement data protection principles and comply with data protection rules.
- **Working with Data Protection Officers (DPOs):** Each EU institution and body must appoint a DPO, who is responsible for ensuring that their institution complies with data protection rules. We work closely with DPOs, providing them with training and support to help them perform their role effectively.

1.2 POLICY AND CONSULTATION

The EDPS acts as an advisor on data protection issues in a wide range of policy areas. We aim to ensure that data protection requirements are integrated into all new legislation, by providing

guidance on proposed legislation to the European Commission, as the institution with the right of legislative initiative, and the European Parliament and the Council, as co-legislators. We use several tools to help us:

- **EDPS Priorities:** Each year, we publish a list of priorities, based on the Commission's work programme. 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 Commission consults the EDPS informally before adopting a proposal with implications for data protection. This allows us to provide them with input at an early stage of the legislative process, usually in the form of informal comments, which are not published.

- **Formal Opinions:** Our formal Opinions are available on our website and are published in the Official Journal of the EU. We use them to highlight our main data protection concerns and recommendations on legislative proposals. They are addressed to all three EU institutions involved in the legislative process.

- **Formal Comments**: Like our Opinions, our formal Comments address the data protection implications of legislative proposals. However, they are usually shorter and more technical, or only address certain aspects of a proposal. We publish them on our website.

- **Court Cases:** We can intervene and offer our data protection expertise before the EU courts either on behalf of one of the parties in a case or at the invitation of the Courts.

- **Cooperation with national DPAs**: We cooperate with national DPAs through the WP29, which provides the European Commission with independent advice on data protection issues and contributes to the development of a harmonised approach to data protection 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 TECHNOLOGICAL DEVELOPMENTS

Many new technologies process personal data, in a range of different and innovative ways. Often, the aim of this data processing is to gain economic or other benefits. It is important that data protection and privacy measures adequately address new technological developments, to ensure that individuals are protected from the risks which these new data processing activities might entail.

The EDPS monitors technological developments and their impact on data protection and privacy. Knowledge and expertise in this area allows us to effectively perform our supervision and consultation tasks. This capacity and competence will only continue to grow in importance, due to the changes introduced by the GDPR and foreseen under the revised Regulation for the EU institutions and bodies. Our activities include:

- **Monitoring and responding to technological developments:** We monitor technological developments, events and incidents and assess their impact on data protection. This allows us to provide advice on technical matters, particularly in relation to EDPS supervision and consultation tasks.

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

- **Keeping track of IT at the EDPS:** As the data protection supervisor for the EU institutions, we should set the standard for data protection compliance. We therefore continually monitor and improve the technology used by the EDPS to ensure that it works effectively and efficiently while remaining in line with data protection requirements. This is particularly important as we look to develop and select tools for new tasks, such as supporting the work of the new European Data Protection Board (EDPB) and the new cooperation procedures introduced by the GDPR.

2. 2017 - An Overview

The EDPS Strategy 2015-2019 outlines our vision of an EU that leads by example in the global dialogue on data protection and privacy in the digital age. It sets out a challenging and ambitious agenda for the current mandate, aimed at establishing an international approach to data protection, designed for the digital era.

In 2017, we reached the mid-point of the current mandate. Though our mid-term review of the EDPS Strategy (see chapter 9) demonstrates the significant progress we have made towards achieving our goals, much work still remains if we are to ensure that our vision becomes a reality.

2.1 DATA PROTECTION GOES DIGITAL

Technology is developing at a rapid pace, changing the way we live our lives in ways we could never have predicted. Though the benefits of technological innovation are evident, it is vitally important that we also consider, and address, the impact of the technological revolution on the rights to privacy and data protection. Data protection must go digital.

The digital environment is determining the way in which we live our lives; not only how we communicate, but also the ways in which businesses operate and in which governments interpret their duty to pursue public interests and protect individuals. However, many new technologies rely on the widespread collection and use of huge amounts of personal data, and while technological innovation has raced ahead, institutional reaction has been slow.

The task we face, as a data protection authority, is to develop creative ideas and innovative solutions that allow society to benefit from new technologies while preserving their rights as individuals. This means making existing principles more effective in practice and integrating them with new principles, specifically designed for the digital age and the data-driven economy.

With the increased focus of the General Data Protection Regulation (GDPR) on technical measures and solutions, such as data protection by design and by default, and the forthcoming application of similar principles to the EU institutions and bodies, the need for data protection authorities (DPAs), including the EDPS, to develop their knowledge and expertise on technology is more important than ever before. Not only the DPAs need to have the relevant expertise, anyone required to take decisions on the processing of personal data must have a better understanding of the possibilities and risks related to technological development.

Our work with the Internet Privacy Engineering Network (IPEN), set up by the EDPS in 2014, is a good example of this (see section 4.4.8). With the principles of data protection by design and by default set to become a legal obligation under the new GDPR, IPEN endeavours to bridge the gap between the legal and IT engineering approaches to data protection and to support the development of the privacy engineering profession.

In 2017, the network organised a workshop in Vienna, aimed at highlighting principles that could be used to ensure an increased level of protection for personal data in the development of new technologies. In addition, with interest in privacy engineering now gaining ground outside Europe, IPEN also collaborated with the Future of Privacy Forum (FPF), the Catholic University in Leuven and Carnegie-Mellon University to organise a Trans-Atlantic workshop. The workshop focused on research and development needs in privacy engineering, particularly in relation to data protection by design and by default.

In addition to our work with IPEN, we have also been working hard to develop our knowledge and expertise on new technologies (see section 4.4.7). This knowledge is vital to ensuring that the data protection community is able to respond adequately to new technological challenges and developments and their implications for data protection and privacy.

As well as continuing to monitor developments in Artificial Intelligence (AI) and robotics, we also examined the privacy implications of connected glasses, Cooperative Intelligent Transport Systems (C-ITS) and the potentially disruptive application of AI and distributed ledger technologies, such as blockchain, to developments in the Financial Technology (FinTech) industry. We hope to present the results of our investigations during the course of 2018.

Data protection does not exist in isolation. It is therefore important that we seek solutions to the challenges of

the digital era in collaboration with others. IPEN is a good example of this, as is the Digital Clearinghouse, an EDPS initiative launched in 2016 to facilitate cooperation in the areas of consumer and data protection (see section 4.4.9). Our aim is to work with regulatory bodies to address questions relating to the concentration of market and informational power. The Digital Clearinghouse, which held its first two meetings in 2017, provides a space for dialogue on how to respond to the digital challenge in a way that ensures that individuals maintain control over their personal information.

In a novel procedural development, in 2017 we received the first formal request for an Opinion from the Council. The request concerned a Commission proposal to extend consumer protection to digital content supplied to consumers, focusing on the misguided notion of providing content *in exchange for* personal data. Our Opinion warned against any new provision introducing the idea that people can pay with their data in the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity (see section 4.4.6).

2.2 FORGING GLOBAL PARTNERSHIPS

Technological development has revolutionised the way in which we share data. Yet while huge amounts of data travel across international borders every day, the laws applying to the protection of personal data are determined at regional or national levels. Evidence of programmes based on the mass surveillance of personal data, which came to light in 2013, provided an excellent illustration of the problem, but the international dimension of data protection has actually been a focus of discussions in the data protection community for years.

The EDPS Strategy highlights the importance of turning discussions into action. We need to develop a global, digital standard for privacy and data protection, centred on individuals, their rights and freedoms and their personal identity and security. Moreover, Europe should be at the forefront of this effort, leading by example as a beacon of respect for fundamental rights.

We made significant progress in this area in 2017. Of particular note is our work on developing an ethical dimension to data protection (see section 4.6). Throughout 2017, the work of the Ethics Advisory Group (EAG), launched at the beginning of 2016, has continued to gather pace, contributing to the broader, international debate that we have been working to promote on the digital environment and its ethical implications. Our efforts will culminate in the 2018 International Conference of Data Protection and Privacy Commissioners (ICDPPC), which will take place in Brussels in October 2018. As co-hosts of the conference, we have chosen the topic of digital ethics as the focus of the public session, and hope to facilitate an open dialogue on this topic between individuals and experts from a range of disciplines.

Our efforts to develop global standards for data protection do not stop at ethics, however. We believe that the EU, when negotiating international agreements, must use these agreements to reinforce the rights of EU citizens, by ensuring that they do not compromise the levels of data protection provided for under EU law. This is particularly important in the case of trade agreements. Traditionally, data flows have not been considered a trade issue. However, recent calls to include legislation relating to data flows in trade agreements prompted EDPS Giovanni Buttarelli to publish a blogpost on the subject in December 2017 (see section 4.5.1). He repeated the long-standing EDPS postion that data protection is not a barrier to international cooperation and that data flows should be kept fully and explicitly out of the scope of the EU's trade agreements.

We also participated in the first EU-US Privacy Shield joint review, which took place in September 2017 (see section 4.5.1). The review aimed to assess the implementation of the Privacy Shield, the framework that facilitates the transfer of data from the EU to the US, to ensure that it does not harm the fundamental rights of individuals. The result was less than satisfactory and, alongside our colleagues in the Article 29 Working Party (WP29), we have committed to following up in 2018, using the appropriate measures, if no action is taken to address our concerns.

Speaking with a single EU voice in the international arena will increase the influence and credibility of the European approach to data protection. For this reason, it is important to continue to work in close cooperation with our colleagues in the national DPAs throughout the EU, whether this be in response to key challenges to data protection, as part of our efforts to ensure effective coordinated supervision, or in our joint preparation for the new legal framework.

2.3 OPENING A NEW CHAPTER FOR DATA PROTECTION

EU data protection rules have long been considered a point of reference for many countries around the world. Maintaining this privileged position, however, requires reforming these rules to ensure that they provide adequate protection for the digital age. While reform should not slow down innovation, it should ensure that the fundamental rights of EU citizens are appropriately safeguarded and rebuild trust in the digital society, which has been eroded by revelations of covert and disproportionate surveillance.

On 4 May 2016, the GDPR was published in the Official Journal of the European Union. This marked a big step towards achieving these goals, but much work still remains before the EU's new data protection framework is complete.

In the EDPS Strategy, we commit to acting as a proactive partner in discussions between the European Commission, Parliament and Council on the data protection reform package. We assumed this role throughout discussions on the GDPR, and have adopted a similar approach to ongoing negotiations on the review of Regulation 45/2001, which sets out the rules for data protection in the EU institutions and bodies, and on the reform of the Regulation on ePrivacy (see section 4.1).

In 2017, we published Opinions on proposals for both Regulations, emphasising the need to ensure consistency with the GDPR. Discussions on the review of Regulation 45/2001 moved to the trilogue stage in November 2017, and we continue to push for an agreement as soon as possible, in line with the legislators' commitment to ensure that these rules are applicable on the same day as the GDPR. This is important in order to ensure that the EU institutions are able to lead by example in the application of the new data protection rules.

We have been working hard to prepare the EU institutions for the new rules. In particular, we have focused on introducing them to the principle of accountability, which will require them to not only comply with the new rules, but also to demonstrate this compliance. We have been working closely with the Data Protection Officers (DPOs) in the EU institutions to help them prepare, but have also reached out to management and to other EU staff members affected by the new legislation.

In our Opinion on ePrivacy, we called for smarter, clearer and stronger rules, while outlining our key concerns. Progress on this legislation has been slower, but we were pleased to note that the European Parliament's report on ePrivacy, which will be used in trilogue negotiations with the Commission and the Council, built on our recommendations. We will continue to follow developments on the ePrivacy Regulation into 2018 and hope to see an agreement as soon as possible.

We also invested a lot of energy in preparations for the GDPR in 2017. This has involved working closely with our WP29 colleagues both on producing guidance relating to key provisions of the GDPR and in setting up the European Data Protection Board (EDPB), for which the EDPS will provide the Secretariat. The EDPB will take over the responsibilities of the WP29, as well as performing other tasks aimed at ensuring the consistent application of the GDPR across the EU. We made significant progress in our preparations for this new responsibility in 2017, selecting a logo, designing a website and establishing a dedicated EDPB sector within the EDPS framework. Building on the collection and analysis of needs of the EDPB secretariat and the national DPAs for the new cooperation and consistency procedures, and on the analysis of technological options, in 2017 decisions on the technical platform were taken and the project for the implementation of this platform started. Preparations will continue throughout the first half of the next year, to ensure that the Board is operational by May 2018.

In addition to preparing for the new legislation, the EDPS Strategy sets us the task of facilitating responsible and informed policymaking (see section 4.4.6). In 2017, our efforts surpassed those of the previous years under the current mandate. Not only did the number of Opinions we issued on EU proposals with data protection and privacy implications increase, we also provided practical guidance for policymakers, through the publication of a Necessity Toolkit. Moreover, two of the Opinions we issued were directly requested by the Council, something that has not happened before. Both observations serve to demonstrate the quality and value of the advice we issue to the EU institutions, and our improving cooperation with the Council in particular.

Meanwhile, in our supervisory role, we took on a new responsibility in 2017: the supervision of Europol (see section 4.2). One of our key challenges in this new role is to ensure that Europol is able to strike the right balance between security and privacy when dealing with data processing for the purpose of law enforcement. We have endeavoured to establish effective working relationships with our colleagues at Europol, ending 2017 with a productive inspection of

their data processing activities. We look forward to building on these foundations in 2018, and hope that Europol can set an example for others by promoting a mature approach to security and privacy.

2.4 INTERNAL ADMINISTRATION

Ensuring that our internal administration and data protection policies are adequate and effective plays an essential role in enabling the institution to reach its goals. This is even more important considering the administrative support we will provide for the EDPB (see section 7.2).

In 2017, we continued our work to ensure that the EDPB receives the human and financial resources necessary to carry out its tasks. This included setting up the EDPB sector and an ambitious plan for recruitment in the first half of 2018. We also put data protection into practice, through the implementation of the EDPS data protection accountability tool, making sure that we, too, are prepared for the new Regulation and are able to set an example for others to follow.

In addition, we have introduced new tools and policies, such as the HR Forward Planning tool and policies on equal opportunities and diversity, all designed to ensure that the EDPS remains an efficient and pleasant work environment.

2.5 COMMUNICATING OUR MESSAGE

Similarly, as our role and responsibilities continue to grow, it is more important than ever that we are able to communicate about our work as effectively and transparently as possible (see section 7.1).

We launched a new website in March 2017, designed to do exactly this. A new-look Newsletter followed soon after, marking the end of our efforts to rebrand and update the image of the EDPS for a new era. Work on creating new websites for the EDPB and the 2018 International Conference is now well underway, with both projects due for completion in 2018.

In addition to this, we have continued to expand our reach, not only through the use of social media and press activities, but also through study visits and events.

With deadlines for the EDPB and the 2018 International Conference approaching, and the role and global presence of the EDPS only continuing to increase, we anticipate another busy year in 2018.

2.6 KEY PERFORMANCE INDICATORS 2017

Key performance indicators (KPIs), established in accordance with the strategic objectives and action plan defined in the Strategy 2015-2019, help us to monitor the performance of our activities and adjust them, if needed, to increase the impact of our work and the efficiency of our use of resources.

The KPI scoreboard on the following page contains a brief description of each KPI and the results on 31 December 2017. In most cases, these results are measured against initial targets.

In 2017, the majority of KPIs met or surpassed their targets, indicating that the implementation of the relevant strategic objectives is well on track and does not require corrective measures.

The following information clarifies the monitoring results of three KPIs:

- KPI 4 analyses the impact of selected EDPS Opinions. This KPI could not be assessed as planned due to delays in the legislative process, which made it impossible to carry out the exercise as planned in relation to the two selected Opinions for 2017 (Directive on digital content and revision of Regulation 45/2001). This KPI is being reconsidered in light of its strong dependence on factors outside EDPS control, such as developments and delays in the legislative process;

- KPI 7 is the composite indicator on visits to the website and Twitter followers. This KPI produced mixed results: while the number of Twitter followers well exceeded the target, the number of visits to the EDPS website was lower than the set target. This is primarily because the figures for 2017 visits to the website only take into account the number of visitors since the launch of the new EDPS website in March 2017. The very positive feedback we received on the new website and the sufficiently high number of visitors allow us to conclude that it remains a valuable online resource for those interested in our work and in data protection in general;

- KPI 8, on staff satisfaction, was not assessed in 2017 as it is linked to the HR survey, a biennial exercise to be carried out again in 2018.

KEY PERFORMANCE INDICATORS		RESULTS AT 31.12.2017	TARGET 2017
Objective 1 - Data Protection goes digital			
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
Objective 2 - Forging global partnerships			
KPI 3	Number of cases dealt with at international level (WP29, CoE, OECD, GPEN, International Conferences) for which EDPS has provided a substantial written contribution	31	10
Objective 3 – Opening a new chapter for EU Data Protection			
KPI 4	Analysis of impact of the input of EDPS Opinions	*N/A for 2017*	
KPI 5	Level of satisfaction of DPO's/DPC's/ controllers on cooperation with EDPS and guidance, including satisfaction of data subjects as to training	92.3%	60%
KPI 6	Rate of implementation of cases in the EDPS priority list (as regularly updated) in form of informal comments and formal opinions	100%	90%
Enablers – Communication and management of resources			
KPI 7 (composite indicator)	Number of visits to the EDPS website Number of followers on the EDPS Twitter account	181 805 9407	2015 as benchmark (195 715 visits to website; 3631 followers on Twitter) +10%
KPI 8	Level of Staff satisfaction	*N/A for 2017*	

Fig. 1. EDPS KPI analysis table

3. Main Objectives for 2018

The following objectives have been selected for 2018 within the overall Strategy for 2015-2019. We will report on the results in the 2018 Annual Report.

Preparing for the EDPB

Under the General Data Protection Regulation (GDPR), the European Data Protection Board (EDPB) is set to replace the Article 29 Working Party (WP29) in May 2018 (see section 4.1.1). Our preparatory work will therefore continue during the first half of 2018 in order to ensure that the EDPB Secretariat is ready to start work from the day the GDPR becomes applicable, and that the proper transitional arrangements are in place for a smooth handover. This work will include ensuring that we have sufficient human and financial resources and that we have established the appropriate working methods. We will also continue our work on the EDPB IT communication system and website. We will maintain our close cooperation with the WP29, both in our preparations for the EDPB and in the drafting of guidelines on the implementation of the GDPR.

Completing the EU data protection framework

In January 2017, the Commission issued proposals for a new Regulation on data protection in EU institutions and bodies, to replace the current rules set out in Regulation 45/2001, and a new Regulation on ePrivacy. At the end of 2017, trilogue negotiations between the European Parliament, the Commission and the Council on the revision of Regulation 45/2001 were underway, while work on the ePrivacy Regulation continued in the Council (see sections 4.1.2 and 4.1.4).

In 2018 we will continue to actively follow the ongoing negotiations and provide targeted input where appropriate. Our aim is to ensure that both Regulations align as much as possible with the principles of the GDPR and are applicable with the least delay possible.

Preparing for the revised Regulation for the EU institutions

The revised Regulation 45/2001 will define the supervisory role and powers of the EDPS and set out the rules we must enforce in the EU institutions and bodies. We will therefore continue to devote considerable resources to ensuring the efficient and effective implementation of these rules (see section 4.1.3). This includes updating our internal procedures to bring them in line with the new Regulation and working with the EU institutions and bodies to help them to implement the new rules. Our aim is to ensure that the EU institutions are able to lead by example in their application of the EU's new data protection package.

Effective supervision of Europol

A new data protection framework for Europol came into force on 1 May 2017, appointing the EDPS as the body's new supervisory authority (see section 4.2). Our new role involves carrying out supervision tasks, including complaint handling, consultations, requests for information, inquiries and inspections. We also provide the Secretariat and cooperate with national supervisory authorities as part of the Cooperation Board. In 2018 we will continue to put in place a framework of efficient supervision, building on the successes and lessons learned from our first eight months of supervision. We will also concentrate on ensuring a high level of protection for individuals, with a particular focus on the principle of accountability. One of our key challenges is to ensure that Europol strikes the right balance between security and privacy when processing data for the purpose of law enforcement.

Putting our IT expertise into practice

We will continue to develop our approach to inspections by focusing on technological aspects, particularly those concerning the EU's large-scale information systems and in the area of security and law enforcement, such as Europol. We also aim to use the EDPS Lab to perform remote inspections of the websites and mobile apps operated by EU institutions. Furthermore, we will continue to facilitate the discussion between technology and legal experts on concepts and methodologies aimed at making data protection by design and by default a reality, as well as encouraging the development of new approaches to the processing of personal data in the organisations under our supervision.

Completing the Security Union

In 2018 we expect to issue Opinions on three upcoming Commission proposals concerning EU borders and security. These will include Opinions on the interoperability of EU information systems (see section 4.3.4), the cross-border access of law enforcement authorities to electronic evidence and cross-border access to and use of financial data by law enforcement authorities. We will also closely follow developments relating to the retention of communications data.

Guidance on technology and data protection

In 2016 we issued Guidelines on the protection of personal data in web services and mobile apps. In 2018, we will issue Guidelines on IT governance and management, as well as cloud computing. We use our technological expertise to support the EDPS in carrying out our roles as an advisor and a supervisor and aim to increase the visibility of our work in this area by revising and issuing guidance and policy advice on specific technologies or methodological approaches, especially those relating to security.

Facilitating the assessment of necessity and proportionality

In 2017 we published a Necessity Toolkit (see section 4.4.6), aimed at providing policymakers with a practical guide on how to apply the data protection principle of necessity. In 2018, we plan to make similar contributions related to the principle of proportionality in EU data protection law, as part of our efforts to facilitate responsible and informed policymaking in the EU institutions.

Data protection goes digital

Article 25 of the GDPR makes data protection by design and by default a mandatory requirement (see section 4.4.8). We plan to raise awareness of the need to apply these principles by issuing an Opinion on the topic in early 2018. In addition, we want to encourage designers to implement Privacy Enhancing Technologies (PETs) in new apps, and plan to do so by providing an award to privacy friendly mobile health (mHealth) apps.

We will also work with the Internet Privacy Engineering Network (IPEN) to raise the profile of privacy engineering. The work of IPEN is vital to ensuring the effective application of data protection by design and by default, bringing together specialists in technology, law and privacy to promote privacy-friendly technology and privacy-aware engineering techniques. Building on successful workshops with representatives from academia, industry and civil society, IPEN cooperation efforts will intensify in 2018.

IPEN will continue to closely monitor technological developments likely to have an impact on data protection and privacy, and will share its findings through the publication of research reports and policy recommendations aimed at keeping the wider privacy, IT and engineering communities informed.

Moving forward with the Digital Clearinghouse

In 2017 we launched the Digital Clearinghouse (see section 4.4.9). The project aims to bring together agencies from the areas of competition and consumer and data protection who are willing to share information and discuss how to enforce rules that support the interests of the individual in the digital space. Further meetings of the Digital Clearinghouse are planned for 2018, which will look to develop the work started in 2017, with the possibility of extending this work to the topics of unfair price discrimination and liabilities of intermediaries.

Micro-targeting for non-commercial purposes

In 2018, we plan to issue an Opinion on voter micro-targeting, online manipulation and personal data. This Opinion will also focus on the use of Big Data in political campaigning and will help determine the data protection challenges related to voter micro-targeting through the use of personalised content, including *fake news*, to influence their voting behaviour.

Integrating ethics into the daily work of data protection authorities

The work of the EDPS and the Ethics Advisory Group (EAG) over the course of the current mandate has raised the profile of digital ethics in the data protection

community. It is now important that we start to integrate ethical insights into our day-to-day work as an independent regulator and policy advisor, and that we cooperate with our colleagues in other data protection authorities (DPAs) to do so. The International Conference of Data Protection and Privacy Commissioners (ICDPPC), which will be hosted in Brussels by the EDPS and the Commission for Personal Data Protection of the Republic of Bulgaria (CPDP) in October 2018 (see section 4.6.5), will provide an excellent forum through which to develop and reinforce this cooperation on an international scale.

Preparing for the International Conference

The work of the EAG will conclude in 2018 with the publication of their report, which will provide an overview of their deliberations. This report will provide a valuable contribution to the discussions that will take place at the 2018 International Conference. In 2018 we will continue our preparations for the International Conference, both in terms of the logistics and programme. Our aim is to facilitate dialogue across a wide spectrum of groups and individuals from a range of disciplines on the topic of digital ethics.

4. 2017 Highlights

Much of our work in 2017 focused on preparing for the new legislative framework. We stepped up our efforts to ensure that the new European Data Protection Board (EDPB) will be ready to take on its responsibilities in May 2018 and continued to work closely with our colleagues in the Article 29 Working Party (WP29) to provide guidance on the General Data Protection Regulation (GDPR). We also provided advice to the legislator on proposals for new rules on data protection in the EU institutions and ePrivacy, while our efforts to prepare the EU institutions for these new rules continued to gather momentum.

Under the Europol Regulation, the EDPS took over responsibility for supervising the processing of personal data relating to Europol's operational activities on 1 May 2017. This new supervisory role represents a new challenge for the EDPS, as we endeavour to ensure that Europol is able to strike the right balance between security and privacy when dealing with data processing for the purpose of law enforcement.

With terrorism and migration still rating high on the EU agenda, in 2017 the European Commission continued to move forward with its plans for a security union. We responded to several new proposals designed to keep EU borders secure, while the public debate on how to balance the need for security with the right to privacy continued. We contributed to this debate with the updated Necessity Toolkit, intended to guide the legislator, while also cooperating with national authorities to supervise the processing of personal data in existing border control systems.

As an advisor to the EU institutions, we issued Opinions for the first time in response to formal requests from the Council, on proposals for a Directive on digital content and on European integrated farm statistics. In our role as a supervisor, meanwhile, we responded to complaints, carried out inspections and issued prior check Opinions, while working with Data Protection Officers (DPOs) and other EU staff members to prepare them for the new rules.

Raising the profile of data protection and privacy globally remains an important goal for the EDPS. In 2017 we contributed fully to European and international discussions on data protection, collaborating with the Council of Europe and the OECD, as well as playing key roles in the International Conference of Data Protection and Privacy Commissioners and the Spring Conference of Data Protection Authorities. We actively monitored and provided advice relating to international data transfers and worked particularly hard to increase cooperation with our European partners, to prepare for new legislative challenges and to ensure that the EU speaks with one voice in the international arena.

A particularly successful area of international cooperation has been our work on digital ethics. With joint responsibility for hosting the 2018 International Conference of Data Protection and Privacy Commissioners, due to take place in Brussels, we have increased our efforts to encourage debate on digital ethics around the world and across disciplines. The work of the Ethics Advisory Group (EAG), which will provide a focus for discussions at the International Conference, has contributed significantly to these efforts.

With new data protection rules due to apply from May 2018 and data protection now a key consideration in all areas of EU policy, the importance of our work will only continue to grow. Achieving our goals and living up to expectations would not be possible without support from our Secretariat. This includes developing new and innovative ways of communicating about our work, as well as maintaining the administrative efficiency of the EDPS workplace (see chapter 7).

4.1 PREPARING FOR A NEW LEGISLATIVE FRAMEWORK

The EU's data protection laws have long been regarded as a gold standard across the world, but in the years since 1995, when the Data Protection Directive first came into force, technological developments have transformed the way we live our lives. If the EU is to continue to live up to its reputation as a global leader in data protection, it needs to open a new chapter for EU data protection by developing a new data protection framework designed for the digital era.

In the EDPS Strategy, we pledged to support this effort. This has meant offering advice and support to the European Parliament, Council and Commission, to ensure that the EU delivers a practical and coherent data protection reform package, and supporting our data protection partners across the EU, to ensure the correct, consistent and timely implementation of new rules.

An integral part of the new data protection package, the General Data Protection Regulation (GDPR), was adopted on 27 April 2016 and will be fully applicable from 25 May 2018. In line with our Strategy commitments, we have been working in close cooperation with data protection authorities (DPAs) across the EU, through the Article 29 Working Party (WP29), to prepare for the GDPR. We have actively contributed to the WP29's efforts to provide guidance on key provisions of the GDPR, in particular as coordinator of the work of the WP29's Key Provisions Subgroup, which has provided the majority of this guidance. Specifically, we served as an active co-rapporteur for guidelines on lead authority, DPOs, profiling, consent, and transparency and provided substantial written input to the guidelines on data portability, Data Protection Impact Assessments (DPIAs) and administrative fines. In addition, we continued to work closely with the WP29 to prepare for our new responsibilities of both providing the Secretariat and acting as an independent member of the new European Data Protection Board (EDPB), which will replace the WP29 under the GDPR.

However, the EU's data protection reform consists of much more than just the GDPR. The new data protection package includes the Directive on data protection in the police and justice sectors, as well as a revised Regulation for the EU institutions and bodies and a new ePrivacy Regulation, both of which are yet to be finalised. We are dedicated to making sure that both new Regulations reflect and uphold the main principles of the GDPR, as well as to ensure that the EU institutions and bodies we are responsible for supervising are prepared for the changes and challenges the new Regulation will bring. Our aim is to ensure that the EU institutions lead by example, setting the standard for data protection practice across the EU, and across the world.

4.1.1 Practical preparations for the EDPB

Among many other things, the GDPR provides for the establishment of the EDPB. The Board will not only take over the responsibilities of the WP29, but will perform many new tasks aimed at ensuring the consistent application of the GDPR across the EU.

The EDPS will act as a member of the EDPB, while also providing its Secretariat. Across all EDPS units and sectors, we are working in close cooperation with our WP29 colleagues to ensure that the EDPB will be able to start work on 25 May 2018, the day on which the GDPR will become fully applicable.

In 2017, we appointed a liaison coordinator tasked with coordinating all EDPS work relating to the preparation of the EDPB Secretariat. This has included working with the WP29 to develop the future EDPB website and to design and choose the future EDPB logo (see section 7.1.4), as well as cooperating with the WP29 to draft a Memorandum of Understanding between the EDPB and the EDPS. In addition, we have contributed to the drafting of the EDPB rules of procedure and helped to define different procedures relating to the consistency mechanism, which aims to ensure consistent application of the GDPR across the EU. We also completed the specification of requirements for the IT system for the EDPB and DPAs, which will support the application of the GDPR, and have started the implementation project for this system, based on a thorough analysis of the technological options

Working under the liaison coordinator, we have now established an EDPB sector, with dedicated office spaces for the staff members concerned. Our work will continue through the first half of 2018 to ensure that the Board is operational by May 2018.

4.1.2 Revising Regulation 45/2001

While the GDPR provides the rules for data protection in businesses and organisations operating across the EU, it does not apply to the EU institutions and bodies, which are subject to their own rules. These rules are currently set out under Regulation 45/2001, but the process of updating them and bringing them in line with the GDPR is well underway.

The new Regulation must ensure consistency with the GDPR through an emphasis on accountability and safeguards for individuals, rather than procedures. Though some deviations from the GDPR might be justifiable, it is important that they are kept to a minimum.

The European Commission adopted a proposal for the updated Regulation on 10 January 2017. On 15 March 2017, we published an Opinion on it. Though we felt the proposal achieved a good balance between the various interests at stake, we also highlighted a number of areas for improvement, particularly in relation to the restriction of the rights of the individual and the need to provide the EU institutions with the possibility to use certification mechanisms in certain contexts.

The Regulation also sets out the tasks and powers of the EDPS. In this respect, we found that the proposal struck a reasonable balance between the interests at stake and reflected the normal functions of an independent data protection authority.

Following the adoption of positions by the European Parliament and the Council, discussions on the revised Regulation entered the *trilogue* phase in November 2017. We called on the European Parliament, the Council and the Commission to reach an agreement on the new Regulation as swiftly as possible, so that the EU institutions can lead by example in the application of new data protection rules.

4.1.3 Coordinating the transition to the new Regulation for the EU institutions

In the EDPS Strategy, we set out our vision of an EU that leads by example as a beacon of respect for data protection and privacy. If we are to achieve this vision, we must start at the level of the EU institutions.

In addition to aligning the rules applicable to the EU institutions and bodies with the principles of the GDPR, the new Regulation will also re-define the role and powers of the EDPS, as the supervisory authority responsible for ensuring that the EU institutions comply with data protection rules. To ensure that we are prepared for the anticipated changes, we established an internal task force to update our internal procedures and help the EU institutions to implement the new rules.

Over the past two years, we have been working with EU institutions at the highest level, in order to prepare them for the new challenges in data protection compliance. Though the new Regulation is yet to be finalised, it is possible to make an educated guess as to what it will involve, based on the Commission's proposal and the content of the GDPR.

In particular, we have focused on the principle of accountability, which requires that the EU institutions are able to demonstrate their compliance with data protection rules. On 26 April 2017, we organised a workshop for DPOs, aimed at helping them to improve accountability in their respective institutions. Throughout the year, we also provided several training sessions for controllers in the institutions, who are responsible for determining how and for what purposes personal data is processed. In addition, we carried out individual visits to a number of EU institutions and bodies, where we met with top management and controllers to raise awareness about their new responsibilities.

We have started work on updating a number of existing Guidelines and policy papers, to bring them in line with the new rules, and we plan to issue new Guidelines on DPIAs, accountability and the rights of data subjects in 2018. Our work on preparing for the new Regulation will continue into 2018, with new and updated guidelines, trainings and accountability visits planned alongside a communications campaign. It is vital that we continue to strengthen our cooperation with the EU institutions to ensure they are prepared to lead by example.

4.1.4 A crucial moment for communications privacy

The GDPR is one of the EU's greatest recent achievements, but without a complementary and effective legal tool to protect the right to the confidentiality of communications, the data protection framework remains incomplete. To fill this void, the Commission published its proposal for a new ePrivacy Regulation on 10 January 2017.

On 24 April 2017, we issued our response. As well as welcoming the proposal and recalling the need expressed in our 2016 Preliminary Opinion for smarter, clearer and stronger rules for ePrivacy, our 2017 Opinion outlined our key concerns. These related to scope and definitions, the need to ensure genuinely freely given consent, the need for clarity about the relationship of the ePrivacy Regulation with the GDPR and the need for privacy by default.

On 27 October 2017, the plenary of the European Parliament approved their Report on the new ePrivacy Regulation. We were pleased to note that the Report, which they will use in their negotiations with the Council and Commission on the final Regulation, follows many of the recommendations provided in our Opinions. It also builds on our recommendations on the proposed parliamentary amendments, which we published on 5 October 2017, as well as the recommendations set out by the WP29, to which we actively contributed as co-rapporteurs.

Importantly, and despite massive lobbying efforts, the Parliament's Report refrains from unduly expanding the legal bases for the processing of personal data specified in the proposed ePrivacy Regulation. Most notably, amendments aimed at allowing the processing of data on the basis of *legitimate interest* were not included in the Report. With few exceptions, the Report specifies that internet companies and communication providers should only be able to process user data with user consent. It also prohibits tracking walls and *take-it-or-leave-it* approaches, helps to ensure that consent is genuinely freely given and requires privacy by default for software settings.

The work in the Council will continue in 2018. We will actively follow the ongoing negotiations and provide targeted input where appropriate.

4.2 SUPERVISING EUROPOL

Europol is the EU body responsible for supporting the law enforcement authorities of the Member States in the fight against serious international crime and terrorism. On 1 May 2017, the new Europol Regulation came into force tasking the EDPS, as the EU's independent data protection authority, with supervising the processing of personal data relating to the operational activities carried out by Europol. The processing of personal data relating to Europol's administrative activities, including personal data relating to Europol staff, is also under EDPS supervision, but is subject to the rules outlined in Regulation 45/2001.

The EDPS takes over this supervisory role from the Joint Supervisory Body (JSB), composed of representatives from the Member States, which had been responsible for supervising data processing at Europol since 1995.

The new Regulation brings Europol supervision fully in line with the requirements of the EU Charter of Fundamental Rights. The EDPS acts as an independent supervisory authority with full-fledged enforcement powers, whose decisions can be challenged before the European Court of Justice. Europol is amongst the first of the EU bodies operating in the Area of Freedom, Security and Justice to be placed under EDPS supervision for data protection matters. We will also act as the supervisor for the new European Public Prosecutor's Office and there is a proposal for the EDPS to be appointed as the supervisor for Eurojust. Supervision of EU institutions, bodies, agencies and information systems in the so-called Area of Freedom, Security and Justice is therefore set to become a core activity for the EDPS.

To help us in our work on Europol supervision, we cooperate closely with national supervisory authorities through a Cooperation Board, an advisory body for which the EDPS also provides the Secretariat. This Board meets regularly to facilitate cooperation between the EDPS and national supervisory authorities on issues requiring national involvement.

In addition, a parliamentary supervisory body, the Joint Parliamentary Scrutiny Group (JPSG), made up of more than 120 representatives from the European Parliament and national Parliaments, has been set up to hold Europol accountable for its activities. We are required to support the JPSG in its tasks.

One of our key challenges in our new role is to ensure that Europol strikes the right balance between security and privacy when dealing with data processing for the purpose of law enforcement. We firmly believe that the idea of a secure and open Europe can only become a reality if we are able to ensure both enhanced operational effectiveness in the fight against cross-border crime and the fundamental rights and freedoms of individuals.

4.2.1 Getting to know Europol

In anticipation of our new role at Europol, an internal EDPS task force was set up in 2016, dedicated to preparing for this role. The task force continued its preparatory activities up until the new Regulation became applicable on 1 May 2017. EDPS staff have followed internal and external training sessions related to Europol supervision, and we have established and maintained regular contact with Europol's Data Protection Function team (DPF), to foster mutual understanding and establish effective communication channels.

On 15-16 May 2017, we organised an operational visit to Europol's premises. This visit helped us to familiarise ourselves with Europol's practices and procedures. We were given full access to Europol premises as well as on-the-spot demonstrations of Europol's data processing activities. We were also given technical presentations, which provided us with an overview of Europol's systems and the layout of their networks.

To ensure we were up to date with the most recent developments in Europol supervision, we also requested an overview of the main recommendations given to Europol by the JSB after their most recent inspections, as well as an update on what Europol had done to address these recommendations.

4.2.2 Keeping in contact with Europol's data protection team

In line with the requirements outlined in the Regulation, Europol has appointed a Data Protection Officer (DPO), who must act independently in the performance of his duties. In order to monitor Europol's compliance with the Regulation, we work closely with Europol's DPO and the DPF team and regularly provide informal advice to the DPF team.

To reinforce this cooperation and ensure it works smoothly, we meet with the DPF and other relevant operational staff on a regular basis. These meetings are an opportunity to discuss any new projects and data processing procedures planned by Europol, as well as other pending issues.

In 2017, we held two meetings with the DPF. These took place in The Hague, on 10 July 2017 and 25 September 2017. We also met the DPF and other Europol staff members in Brussels on 6 and 7 November 2017. So far, these meetings have proved a valuable tool, helping us to anticipate consultations on data processing and to define and plan for future activities, such as inspections or inquiries. Our next meeting is planned for February 2018.

4.2.3 Keeping up to date with new analysis projects

In accordance with the Europol Regulation, Europol can process personal data for operational analysis, that is, to support criminal investigations and criminal intelligence operations carried out by law enforcement authorities in the Member States, but only in the context of *operational analysis projects*.

Each operational analysis project focuses on a specific crime area, such as child pornography, cybercrime, drug trafficking, organised criminal groups, property crimes or terrorism. For each project, Europol must define the specific purpose, the categories of data and the individuals involved, the participants (Member States, non-EU countries, international organisations), how long the data will be stored and the conditions for access and any proposed transfer or use of the data concerned. The EDPS must also be informed of this.

Europol informed the EDPS about its portfolio of 28 existing operational analysis projects on 1 May 2017 and about amendments to the portfolio, as required by the Europol Regulation. In 2017, we were consulted informally about two new analysis projects prior to their actual creation.

4.2.4 Giving our opinion on Guidelines

As the supervisory authority for Europol, we are responsible for providing them with advice on all matters concerning the processing of personal data. This includes proposals for internal rules or administrative measures relating to the protection of the fundamental rights of individuals or the transfer and exchange of personal data. We issue our recommendations in the form of an Opinion. On 6 July 2017, we published our first Europol Opinion, which

concerned Europol's Integrated Data Management Concept (IDMC) Guidelines.

The IDMC Guidelines were provisionally adopted by Europol on 1 May 2017, pending EDPS approval. They specify:

- the conditions under which personal data might be temporarily processed in order to determine whether it is relevant to Europol's tasks;
- the procedures for processing personal information;
- the requirements for processing personal information for cross-checking, strategic or thematic analysis, operational analysis or for facilitating the exchange of information.

The guidelines therefore provide the procedures according to which Europol must carry out all future processing of personal data under the Europol Regulation.

In our Opinion, we made 16 recommendations. Our main concern was the need to further clarify the different purposes for which Europol can process the same data in the same database, for example, simultaneously processing data for operational and for strategic analysis. This issue is important because different data protection safeguards apply depending on the purpose for which data is processed. In the case of Europol, this refers to the type of intelligence service or product Europol plans to deliver to the national law enforcement authorities concerned.

Europol promptly implemented the recommendations made by the EDPS in the revised version of the IDMC Guidelines, which were adopted by Europol's Management Board on 13 December 2017. Europol has also promised to work on clearly defining and streamlining procedures and their respective data protection safeguards, such as data retention periods, for each type of analysis product or service they provide.

4.2.5 Inspecting Europol

From 12-15 December 2017, we carried out our first inspection of Europol. Taking advantage of the opportunity provided in the Europol Regulation, we conducted a joint inspection alongside an expert from the Italian data protection authority (DPA), who participated in the last JSB inspections. This allowed us to ensure continuity with the JSB's supervision activities.

This first inspection aimed to check on the implementation of pending recommendations formulated by the JSB, as well as to assess Europol's overall level of compliance with the new legal framework. Europol's Regulation requires the organisation to implement a new approach to data protection, based on regulating data uses, such as cross-checking and strategic, thematic and operational analysis. We therefore paid particular attention to the processes and tools used to process personal data and to produce intelligence products and services.

The legal part of our inspection focused on Europol's data lifecycle. First, we looked into the data intake process at Europol's Front Office, where all incoming information is subject to a legality check and directed to the relevant operational analysis project. We then examined the processing activities conducted in the criminal areas of migrant smuggling and heroin trafficking, and scrutinised the data review process. Finally, in order to assess compliance with the processing of administrative data under Regulation 45/2001, we also inspected Europol's internal auditing system, as a tool used to monitor the activities of Europol staff.

The technical part of the inspection focused on three items: an audit of the Information Security Management Programme applied by Europol; an assessment of the time limits set for the storage and erasure of personal data under the Europol Regulation and, more specifically, the existing technical rules applied in all automated systems that process operational data; and an audit of the logs Europol must maintain for all personal data processing activities under the Europol Regulation.

Throughout the inspection, we were able to rely on the collaboration of Europol's DPF team and the Europol staff involved. The results of our inspection and our recommendations will be communicated to Europol in due course.

4.2.6 Carrying out prior consultations

Prior consultations are required whenever a new data processing activity planned by Europol involves the processing of sensitive data or might present a specific risk to individuals. Based on the facts submitted by Europol, the EDPS is required to examine the proposed processing operation in relation to the data protection safeguards laid down in the Europol Regulation and all other relevant data protection principles and rules. We then provide them with recommendations that need to be implemented in order to ensure compliance.

In 2017, we received three prior consultations. We will provide Europol with the relevant feedback in 2018.

4.2.7 Dealing with complaints

Another of our supervisory responsibilities is to hear and investigate complaints from individuals who believe that Europol has mishandled their personal data. We investigate all admissible complaints, in consultation with the relevant national supervisory authorities in the Member States, and adopt a decision.

In 2017, we received only two complaints. One was deemed inadmissible, as it related to a request for access to data that Europol, at the time of receiving the complaint, had not taken a decision on.

The other complaint was considered admissible and was still under investigation at the end of 2017. It relates to a claim that Europol did not provide access to personal data when requested to do so by the individual concerned.

4.2.8 Meeting with the Cooperation Board

Europol's work requires close collaboration with relevant national authorities in the Member States. While it is the task of the EDPS to supervise the processing of personal data by Europol, it is the task of each national DPA to oversee the processing of personal data by their respective national law enforcement authorities. To perform our supervisory duties at Europol it is therefore essential that we are able to cooperate effectively with the national DPAs.

To help us with this, the Europol Regulation provides for the establishment of a Cooperation Board, for which the EDPS provides the Secretariat. The Board has an advisory function and provides a forum to discuss common issues as well as to develop guidelines and best practices.

The Board meets at least twice a year and is composed of representatives from the relevant national DPAs and the EDPS. In 2017, these meetings took place on 14 June 2017 and 16 November 2017. At the June meeting, the Board adopted its rules of procedure and elected a Chair and Vice-Chair.

4.2.9 Ensuring sound cooperation at management level

On 3 October 2017, EDPS Giovanni Buttarelli visited Europol to share his views on our supervisory role with the Europol Management Board.

In his speech, he echoed the EDPS Strategy by referring to the importance of moving to a data protection approach based on accountability, specifically the ability of Europol as an organisation to proactively and internally ensure and demonstrate compliance with the principles and rules for the protection of personal data. He also emphasised the importance of a risk-based approach to data protection, stressing that this involves effective documentation of data processing activities as well as the use of risk assessments, Data Protection Impact Assessments (DPIAs) and requests for consultations from the EDPS where necessary.

Mr. Buttarelli also highlighted the importance of effective cooperation with national DPAs, whose work is inextricably linked with the work of the national law enforcement authorities who cooperate with Europol. He made specific reference to the importance of joint inspections, the first of which took place in December 2017.

Lastly, the EDPS called for a creative approach to applying the new legal framework. Though the EDPS has extensive experience working as a supervisory authority for the EU institutions, we recognise that the task of supervising Europol holds its own unique challenges. This is because of the impact of Europol's processing operations on citizens.

4.2.10 The Joint Parliamentary Scrutiny Group (JPSG)

As part of its role, the JPSG requests, at least once a year, a meeting with the EDPS to discuss Europol's compliance with the rules and principles relating to the protection of personal data.

The first meeting of this group took place on 9 October 2017. EDPS Giovanni Buttarelli was requested to appear at the meeting to discuss the protection of personal data with regard to Europol's activities.

In his speech, the EDPS provided an outline of our activities since taking over responsibility for Europol supervision on 1 May 2017, as well as explaining our approach to Europol supervision, based on the accountability principle. He also replied to all questions from the representatives from the European Parliament and national Parliaments.

4.3 SECURITY AND EU BORDERS

In the EDPS Strategy, as part of our pledge to opening a new chapter for data protection, we commit to facilitating responsible and informed policymaking in all cases where EU legislation has a notable impact on privacy and data protection, and to promoting a mature conversation on security and privacy. In the case of EU border and security policy, these objectives are inseparable.

In recent years, the Commission has proposed several initiatives aimed at ensuring EU borders, both on land and online, remain safe and secure, and 2017 was no exception. Though we support these efforts, it is vital to ensure that all proposals fully respect the fundamental rights of those concerned.

Through providing appropriate legal analysis, guidance and recommendations, we aim to ensure that policymakers are able to make informed decisions on EU border and security policy, which strike a balance between the need for greater security, both online and offline, and the right to data protection.

4.3.1 Effective supervision of large-scale information systems

The EU uses several large-scale IT databases to help maintain control over its external borders and make cooperation between EU police authorities easier. They allow national authorities, and in some cases EU bodies, to exchange information relating to borders, migration, customs, and police investigations. The EDPS is responsible for supervising the processing of personal data in the central units of these databases, the majority of which are hosted by the EU's Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA). The national authorities feeding information into these systems are responsible for ensuring the accuracy of

this information and are supervised by their respective national data protection authorities.

One of our supervisory duties is to carry out regular inspections of the central units of the various databases. Not only do these inspections allow us to follow-up on data protection compliance, they also provide us with an opportunity to work directly with eu-LISA to improve accountability in the management of these databases, in line with our Strategy objectives.

On 7 December 2017, we issued a report relating to an on-site inspection we carried out on Eurodac in 2016. Used to identify asylum seekers, the database contains millions of fingerprints, which must be stored and secured appropriately. In our report, we outline a number of recommendations, which we will continue to follow-up on in the coming months.

4.3.2 Coordinated supervision of large-scale information systems

The EU's large-scale information systems consist of a central unit and national units. While the EDPS acts as the supervisory authority for the central units, the national supervisory authorities are responsible for their respective national units. Cooperation, or coordinated supervision, helps to ensure that all supervisory authorities involved adopt a consistent approach to the supervision of these databases. The EDPS Strategy makes an explicit reference to the importance of this approach.

We meet regularly with representatives from the national data protection authorities (DPAs), as part of distinct supervisory groups dedicated to each database, known as Supervision Coordination Groups (SCGs). In 2017, meetings took place in both June and November for the Eurodac database, the Schengen Information System (SIS II) and the Visa Information System (VIS), and in April for the Customs Information System (CIS). The EDPS plays two different roles in these groups, participating as a full member, in our role as the supervisory authority for the central units, and providing the Secretariat for the groups under the authority of the respective Chairs.

Summaries and other relevant information relating to each of the meetings are published in a dedicated section of the EDPS website. The SCGs will meet again in 2018 as part of our ongoing commitment to ensuring effective, coordinated and consistent supervision of these important databases.

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

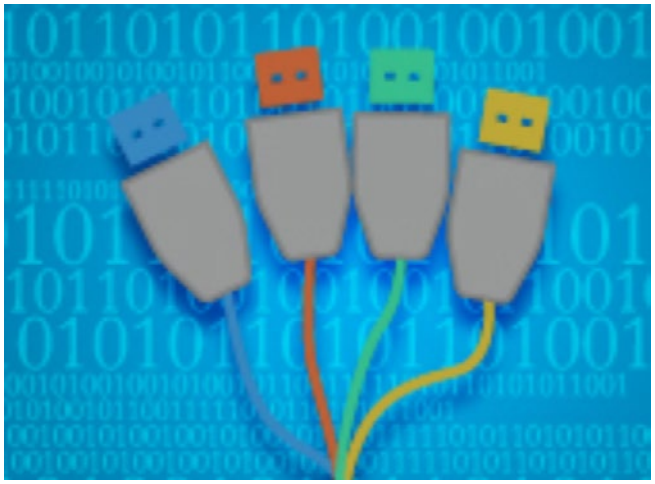
Since its establishment in 2011, eu-LISA has gradually been entrusted with the operational management of the Schengen Information System, the Visa Information System and Eurodac. After four years of operation, the European Commission conducted an evaluation and in June 2017 they published a Proposal for a Regulation on eu-LISA.

Under the proposal, eu-LISA would be entrusted with the operational management of existing and future large-scale IT systems in the area of freedom, security and justice, as well as the development of some features related to the interoperability of these systems (see section 4.3.4). The agency would also be required to carry out research activities and to develop, manage and host a common IT system for Member States interested in a centralised solution for implementing technical aspects of EU legislation in the area of freedom, security and justice.

On 10 October 2017, we issued an Opinion on the proposal. As the supervisory authority for eu-LISA, we recommended that the Commission conduct a detailed impact assessment to determine how the proposal might affect fundamental rights. In particular, we specified that the assessment should focus on the issues associated with concentrating all EU large-scale IT systems in one agency and should take into account the broader legal context, including other ongoing legislative proposals relating to large-scale IT systems.

We also recalled that no legal framework currently exists relating to the interoperability of large-scale IT systems in the EU, and therefore recommended that references to interoperability be removed from the proposal. In addition, the provision allowing for the possible establishment of a central solution for the decentralised systems on the basis of a delegated agreement between eu-LISA and a group of Member States should also be removed, as such an agreement

cannot, under any circumstances, provide a proper legal basis for such a crucial change to the system's architecture.



4.3.4 A coherent approach to borders and security

On 6 April 2016, the Commission published a communication on border management and security in the EU. Among other things, the communication mentions the need to improve the interoperability of the large-scale IT databases used to manage EU borders and facilitate police cooperation.

Interoperability refers to the ability of these databases to communicate and exchange information. Throughout 2017, the EDPS participated in the High Level Expert Group on Information Systems and Interoperability and on 17 November 2017, we published a paper setting out our views and concerns. While we expressed our support for developing a more coherent approach to border management and cooperation, we stressed that any new measure needs to be carefully considered and must ensure full respect for data protection rules.

Interoperability could help increase the efficiency of information sharing in the EU and may even act in the interest of data protection, by helping to ensure that the data held in these systems is up to date. However, making the exchange of data technically feasible would likely provide a powerful impetus for the development of new data processing activities involving the exchange or cross matching of data. As a clear legal basis for carrying out such activities does not currently exist, a new legal basis for processing would need to be established, in full compliance with the EU Charter of Fundamental Rights.

To move forward with the current debate on interoperability, and to help establish a coherent and long-term approach to EU border management and security, we encouraged the Commission to clearly define the problems interoperability aims to solve. Accordingly, they must also set out the specific categories of data to be processed and the purpose for doing so.

4.3.5 Assessing the EU's approach to visa-exempt travellers

On 6 March 2017 we issued an Opinion on the proposed European Travel Information and Authorisation System (ETIAS). The proposal would require visa-exempt travellers to undergo a risk assessment with respect to security, irregular migration and public health before entering the EU.

As the information gathered will be used to grant or deny individuals access to the EU, it is vital that the definition of what constitutes a risk is clearly defined and that reliable methods are used to determine in which cases a risk exists. This is particularly important in relation to the proposed introduction of screening rules, a profiling tool that would enable the ETIAS system to single out individuals suspected of posing a risk. Profiling techniques, as with any other form of computerised data analysis, raise serious technical, legal and ethical questions, related to their transparency and accuracy, which is why we called on the Commission to produce convincing evidence of the need to include and use them in the ETIAS system.

We also stressed the need to conduct a thorough assessment of the impact this proposal will have on the rights to privacy and data protection, to determine whether the measures proposed, and the implications they have for the right to data protection of the individuals concerned, are truly necessary, given the resources already available to the EU in this area.

Border management and law enforcement are distinct objectives, with different implications for data protection

and privacy. It is important to ensure that the EU is better able to address the challenges of migration, borders and refugees, but this cannot come at the expense of protecting fundamental rights. A balance must be found between the two in order to ensure a consistent and effective approach to EU border policy.

@EU_EDPS

.@Buttarelli_G #ETIAS involves visa-exempted collection of #migration #security & #health #data. Big short-term challenges for EU legislator

4.3.6 Encouraging a consistent approach to criminal records

The current European Criminal Records Information Service (ECRIS) is primarily used to facilitate judicial cooperation between Member States, through the exchange of information relating to criminal convictions.

In 2016, the Commission proposed a Directive on ECRIS aimed at improving this system, on which the EDPS issued an Opinion. They wanted to make it easier for Member States to exchange information on non-EU citizens, referred to as third-country nationals (TCN). In 2017, the Commission proposed a Regulation on ECRIS-TCN, designed to complement the Directive and address some of the technical problems encountered in its application. Most notably, they proposed changing the system used to identify which Member States hold information on criminal convictions relating to non-EU citizens from a decentralised system to a centralised system.

In our Opinion of 12 December 2017, we acknowledged the need to develop a more efficient system for exchanging information on the criminal records of non-EU citizens. At the same time, we stressed that any proposal to update the current system must ensure consistency with the EU Charter of Fundamental Rights and the Lisbon Treaty, and fully respect data protection principles.

As the original ECRIS legislation was developed before the Charter and the Treaty came into force, any plans to amend it must bring ECRIS and ECRIS-TCN up to the standards set in these documents. This means clearly defining for what purposes the data stored in these databases will be used and establishing that these purposes are both necessary and proportionate. Any difference in the treatment of the personal data of non-EU citizens and EU nationals must also be demonstrably justifiable.

The proposal involves the establishment of a central database containing fingerprints and facial images, which would be hosted by eu-LISA alongside the majority of the EU's other large-scale databases. The Commission must therefore also conduct a thorough impact assessment to determine whether this represents the least intrusive way of identifying which Member States hold information on the criminal convictions of non-EU citizens. Moreover, as the data concerned is of a particularly sensitive nature, it must only be processed if it is strictly necessary to do so.

@EU_EDPS

#EDPS calls for consistency in #EU approach to #criminal records - Read Opinion http://europa.eu/!YK84rP on #ECRIS system

4.3.7 Observing Schengen

The Schengen area of border-free travel is one of the EU's most notable achievements, but its success depends on a collaborative effort from all states involved. One measure designed to ensure that states adequately implement Schengen rules are regular peer review exercises, known as Schengen evaluations (SCHEVAL).

The European Commission coordinates these peer evaluations, which are carried out by experts from the Member States. The EDPS can also participate as an observer in the evaluation teams for the data protection part, and has so far participated in the SCHEVAL exercises for ten Member States. Our regular inspections and audits of the central SIS and VIS databases (see section 4.3.1) mean that we are able to offer a different and complementary perspective on the SCHEVAL process, which is of clear added value in the supervision, enforcement and promotion of data protection in this

highly sensitive area. In 2017, we took part in the evaluations of Denmark, Sweden, Portugal and Spain.

The data protection aspect of the evaluation assesses competent authorities' compliance with data protection rules, including the security of the SIS and VIS information databases; the independence, role and powers of the national data protection authority; public awareness of Schengen and international cooperation.

4.3.8 Ensuring privacy-friendly protection from cyber-attacks

In a Eurobarometer survey published in September 2017, 87% of respondents considered cybercrime to be an important challenge to the internal security of the EU, while the misuse of personal data was cited as the most significant concern for internet users.

On 13 September 2017 the European Commission and the EU's High Representative for Foreign Affairs and Security Policy proposed a set of measures aimed at increasing EU resilience to cyber-attacks. Referred to as the Cybersecurity Package, they cited the need to establish a system of EU cyber deterrence and criminal law that would better protect people, businesses and public institutions within the EU. On 18 October, the Commission adopted a report on the Security Union, elaborating on some of these initiatives.

The proposed measures include:

- reinforcing the role of the European Network and Information Security Agency (ENISA);
- establishing a European cybersecurity certification framework to create a level playing field within the EU;
- introducing more effective deterrence measures, focusing on the detection, traceability and prosecution of cyber criminals.

On 15 December 2017, we issued formal comments on the proposed policy package. We also plan to provide recommendations on the specific legislative initiatives proposed by the Commission, in order to ensure that they are not only effective, but that they guarantee the protection of fundamental rights, including the rights to privacy and data protection.

Adequate cybersecurity is necessary to protect privacy and personal data, but it is particularly important to focus on prevention: while an effective response is necessary, it is even better to avoid becoming the victim of a cyber-attack in the first place. In cases where the same tools are used to ensure cybersecurity and data protection, such as certification and incident notification, organisations will be subject to both cybersecurity and data protection rules. It is therefore important to ensure that this does not lead to confusion or contradiction.

We particularly appreciated the Commission's commitment to not weaken or undermine the strength of encryption. Trustworthy encryption capabilities are critical for digital markets and societies, as they protect data and help to inspire confidence in online services and cybersecurity tools. Any further measures developed to protect against cybercrime and the processing of personal data must be developed and applied with full respect for the data protection principles of necessity and proportionality.

It is also important to bear in mind that the tools we develop to counter cyber-attacks may be used against us if they ever fall into the wrong hands. Echoing our previous warnings, we urged the Commission to take this into account in relation to the Cybersecurity Package.

4.4. ON THE GROUND

Accountability refers to the ability of organisations to not only comply with data protection regulations but to also be able to demonstrate this compliance. The emphasis on accountability in the General Data Protection Regulation (GDPR), and its inevitable inclusion in the new Regulation applying to the EU institutions, marks an important shift in the EU's

approach to data protection, forcing organisations to take full responsibility for ensuring compliance with data protection rules. Ensuring that the EU institutions set the example in the application of accountability is a key action point in the EDPS Strategy, integral to the opening of a new chapter for data protection.

Over the past few years, we have systematically increased our efforts to raise awareness within the EU institutions about accountability, as well as other important changes that the new Regulation will bring, such as Data Protection Impact Assessments (DPIAs), data breach notifications and data protection by design and by default. This has involved working closely with the Data Protection Officers (DPOs) in the institutions, but also with management and other staff members involved in the processing of personal data.

In addition, we must also fulfil our obligations as a supervisory authority for the EU institutions. This includes issuing recommendations to individual institutions in the form of prior-check Opinions, dealing with complaints and carrying out regular visits and inspections.

The EDPS Strategy also sets us the task of facilitating responsible and informed policymaking, and in our capacity as an advisor to the EU legislator we endeavour to make this happen. In fact, our efforts in 2017 surpassed those of the previous years under the current mandate. Not only did the number of Opinions we issued on EU proposals with data protection and privacy implications increase (in 2017 we issued 11 Opinions, six sets of formal comments, recommendations on the ePrivacy Regulation, and a reflection paper on interoperability), we also provided practical guidance for policymakers, through the publication of a Necessity Toolkit. Moreover, two of the Opinions we issued were directly requested by the Council, something that has not happened before. This is not only a clear sign of our improving cooperation with this institution, but also an indication of the quality and value of our Opinions.

As technology continues to develop apace, we have looked to identify cross-disciplinary solutions to data protection problems, another of our Strategy aims. Some particularly good examples of this are our work with regulatory bodies to establish the Digital Clearinghouse and our work to bridge the gap between legal and IT engineering approaches to data protection through the Internet Privacy Engineering Network (IPEN). In a digital world, we believe the need to work across disciplinary boundaries is increasingly important if we are to develop practical solutions to the new challenges we face.

4.4.1 The DPO function: EU institutions leading by example

DPOs from the EU institutions and bodies meet twice a year with the EDPS to reinforce collaboration and exchange practical experiences. With new data protection rules for EU institutions and bodies planned to come into force alongside the GDPR in May 2018 (see sections 4.1.2 and 4.1.3), these meetings are an excellent opportunity for us to help the EU institutions with their preparations. In 2017, the meetings took place at the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), in Tallinn, Estonia and the European Medicines Agency (EMA) in London.

At both meetings, we focused on making sure that DPOs have the knowledge and resources needed to lead by example in their application of data protection law. We continued our discussions on DPIAs, providing DPOs with guidance on when a DPIA might be required and how to document a DPIA in practice. This complemented our work on helping EU bodies to increase their accountability, which, as one of the action points highlighted in the EDPS Strategy and an inevitable part of the new Regulation, has been a focus of our work over the past few years.

In Tallinn we also addressed the issue of individuals' rights, which will be strengthened under the GDPR and the proposed Regulation, while in London we organised a session on data breach notifications, discussing views on possible procedures and presenting draft guidance, all based on practical scenarios.

As we approach May 2018, we will continue to work closely with our DPO partners to make sure that they are ready when the new rules come into force.

4.4.2 Reinforcing the accountability of EU institutions

Working directly with the EU institutions to prepare them for the new Regulation (see section 4.1.3) has been a specific focus of our work in 2017. In particular, we have concentrated on raising awareness about the new principle of accountability, as well as providing concrete recommendations on how to prepare for the new rules in a timely manner.

In 2017, we organised three participatory workshops with DPOs, focused on these topics. These included an interactive discussion with DPOs on the concept of accountability, which took place at the EDPS offices on 26 April 2017, as well as the DPO meetings in Tallin and London (see section 4.4.1). These workshops were accompanied by two formal letters, from EDPS Giovanni Buttarelli and Assistant Supervisor Wojciech Wiewiórowski, to the top management of each of the EU institutions and bodies, to help them anticipate the upcoming changes.

Since managers working at the EU institutions will be particularly affected by the transition to accountability, we also organised three training sessions for heads of unit and heads of sector, which took place at the European School of Administration in Brussels. We recorded one of these sessions and sent it to all EU institutions and bodies, to be used as an internal training tool.

Our aim has been to target all professional levels of the EU institutions that will be directly affected by the transition to accountability and help them to prepare appropriately. This proactive approach is particularly important considering the limited amount of time EU institutions will have to prepare for the new rules. Our efforts will continue into early 2018, with further training and guidance planned.

4.4.3 Encouraging accountability in IT management

The EU institutions rely on information systems and databases to perform a range of operational and administrative tasks, many of which involve the processing of personal data. Some of this processing takes place in shared pools of configurable computing resources, such as cloud computing services, which help the institutions to reduce costs and increase their flexibility. To help staff in the EU institutions ensure that personal data is adequately protected, the EDPS is developing Guidelines to strengthen their accountability in relation to the development, operation and maintenance of the databases used.

Throughout 2017, we have been working with IT staff and DPOs in the EU institutions to develop these Guidelines. This has included conducting workshops on the topic at the DPO meetings in Tallinn and London. We have focused on the deployment of cloud computing services in particular, with the aim of enabling the EU institutions not only to comply with their data protection obligations, but also to demonstrate their compliance in line with best practices and the GDPR.

Under the GDPR, it will become a legal requirement for designers and developers to incorporate data protection by design into new technologies. This approach will help to develop more privacy-friendly IT systems, and therefore make it easier for the EU institutions to ensure that personal data is protected.

4.4.4 Protecting privacy in the EU institutions

Health and data protection in the EU institutions

In 2017, we addressed two complaints concerning the processing of medical data. The rules that EU institutions and bodies must follow when dealing with such data are set out in Article 10 of Regulation 45/2001. We also issued Guidelines on the topic in September 2009, designed to help the EU institutions comply with their obligations under the Regulation.

The first complaint concerned the processing of medical data to facilitate disciplinary proceedings relating to suspected fraud. It involved analysing whether, under Regulation 45/2001, the EU body concerned had the right to access medical data linked to the reimbursement of medical expenses, stored by a third party, and transfer it to the State Prosecutor.

We concluded that, under the right to information, the EU body should have informed the relevant staff members of both actions and could not claim that doing so would have involved a disproportionate level of effort. For fraud investigations involving medical data, only the relevant medical advisers should have access to this data. DPOs should also be involved in internal disciplinary procedures, especially when they involve the special categories of personal data outlined in Article 10 of the Regulation.

The second case concerned a breach of confidentiality. The EU body concerned disclosed medical data to a third party in order to check the validity of a medical certificate. Though the EU Staff Regulations may justify this action, they also specify that the individuals concerned must be informed of the relevant legal basis under which this data will be processed and that the validity of a medical certificate might be checked. Changing the purpose for which medical data is processed, as occurred in this case, also constitutes a breach of Article 6 of the Regulation, which specifies that this is only possible if expressly provided for in the internal rules of the relevant EU body.

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 2017, the EDPS received 141 complaints, a decrease of approximately 19% compared to 2016. Of these, 116 complaints were inadmissible, the majority relating to processing at national level as opposed to processing by an EU institution or body.

The remaining 25 complaints required in-depth inquiry, a decrease of 7% compared to 2016. In addition, 37 cases submitted in previous years were still in the inquiry, review or follow-up phase on 31 December 2017 (one in 2011, two in 2012, one in 2013, seven in 2014, eight in 2015 and eighteen in 2016). In 2017 we issued 33 complaint decisions.

When the professional becomes personal

Information relating to a registered company, or *legal person*, especially when connected with additional data, can make it possible to identify the individual, or *natural person*, associated with the company. For this reason, information about a registered company can, in certain cases, be considered personal data. The EDPS dealt with two complaints in 2017 relating to company data stored in EU databases.

The first concerned the email address used to register a company in an EU database. The complainant alleged that it had been accessed unlawfully by, or made available to, third parties, and was then used for unsolicited commercial communication (spam).

We found that the data had been processed according to the rules set out in Article 5(a) of Regulation 45/2001, and judged that the EU institution responsible for the database had taken appropriate measures to address the complaint. However, we also recommended that the EU institution move forward with implementing anonymisation techniques to better protect the data stored in the database and advised it to amend the relevant data protection notices to ensure that they provide information on the limited availability of data and on any anonymisation techniques used.

The second complaint concerned an individual whose company is registered in the VAT Information Exchange System (VIES on-the-web). VIES is a search interface which facilitates cross-border economic transactions by making it possible to check the validity of the VAT identification numbers of companies registered in the EU. Our investigation found that the EU institution responsible for VIES had put in place adequate measures to prevent, detect, and stop illicit use of the database.

Though VIES is operated by an EU institution, its content is taken from the national VAT registries in the Member States. These are maintained by the respective national tax administrations and the information recorded by each depends on national law. Only the tax administration that issued the VAT number is able to delete or alter the personal data found in their national registries, and which therefore appears on VIES, and personal information can only be accessed in VIES by searching for a VAT number. Supervision of data processing in this case is therefore the responsibility of the national data protection authority (DPA) of the country in which the company is registered.

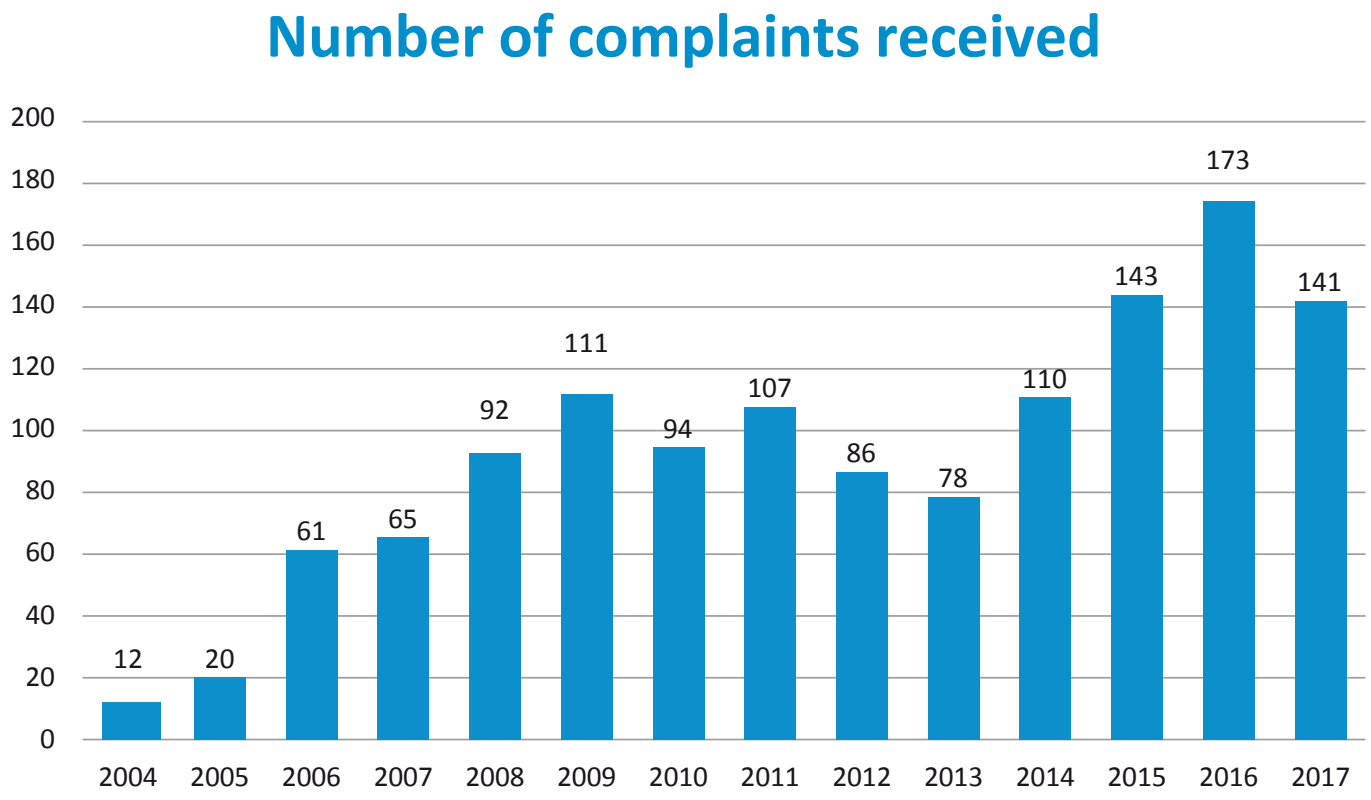


Fig. 2. Evolution of the number of complaints received by EDPS

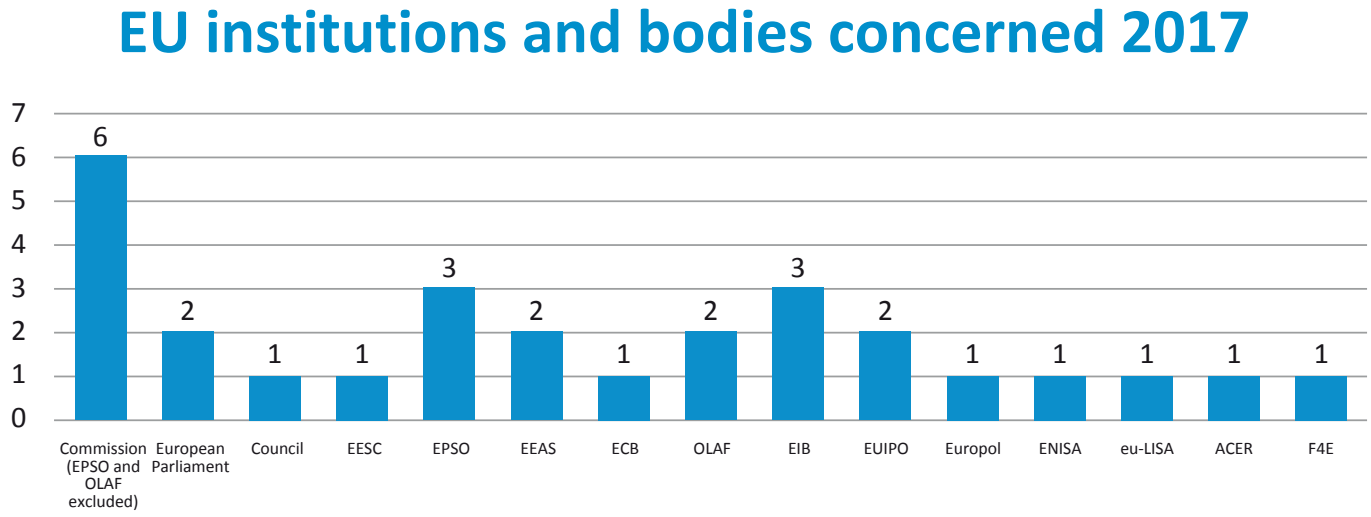


Fig. 3. EU institutions and bodies concerned by complaints received by EDPS

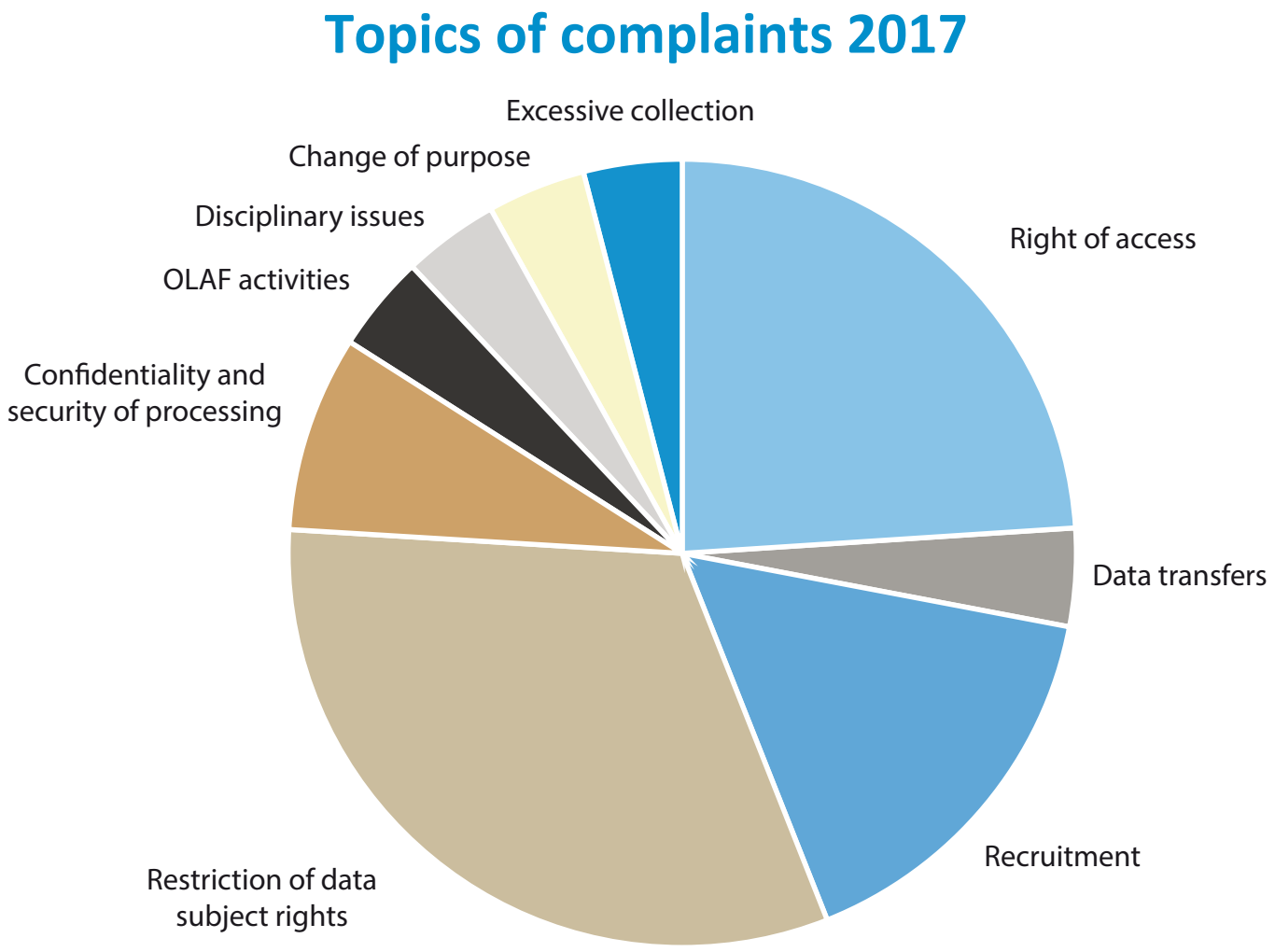


Fig. 4. Type of violation alleged in complaints received by EDPS

Finding a balance between transparency and data protection

It is not always easy for public institutions to ensure they strike an appropriate balance between the need for transparency and the need for data protection. In 2017, we dealt with a complaint relating to a letter sent by an individual to a Commissioner, which was published in the *Cabinet Register On Line* (CAROL). CAROL is a platform used to increase public transparency through the publication of letters sent to the Commissioner by companies.

The case is a good example of how to apply data protection safeguards without unduly compromising transparency. The letter in question was published in CAROL as it was considered to have been sent by a *legal person*, or company representative. However, the individual who sent the letter argued that they sent it in their capacity as a *private* citizen and asked for it to be removed, which the Commissioner's Cabinet agreed to do.

We investigated the matter and adopted a position consistent with similar cases we have dealt with in the past, reminding the Commissioner's Cabinet of the need to also apply certain data protection safeguards in relation to the publication of documents concerning companies. We also recommended that the Cabinet publish a specific privacy statement for CAROL and consider anonymising references to the names of individuals, depending on the case. Lastly, we advised them that any sensitive data must be deleted before a letter can be published, unless the consent of the individual to whom this data relates is provided.

The Commissioner's Cabinet adapted the online register accordingly.

A healthy approach to data protection

In 2017 we received a complaint from a person who recognised a picture of her deceased husband on tobacco packaging. This image is one of the images included in the Annex to the Commission's Delegated Directive establishing a library of mandatory picture warnings to be used on tobacco products. Other individuals, from different countries, made similar claims, which were reported on by the press.

After carrying out a full investigation, we concluded that the individual who appeared in the image in question was not actually the husband of the complainant, but a different person, the image of whom the Commission was able to document they had consent to publish.

The case related to both the right to image and the right to the protection of personal data, and the Commission's obligation to respect these rights. If it had not respected these rights, the Commission would have exposed itself to severe reputational risk. Though we found the Commission to have acted in accordance with data protection rules, we recommended that they add additional information to the relevant consent forms relating to the picture rights, signed by the relevant person. We also stressed that the Commission DPO must be notified of any plans to collect and process the data concerned.

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 2017, we received 124 notifications for prior checking, almost twice the number we received in 2016. We issued 58 prior check Opinions, an increase of approximately 11.5% from 2016. Of these, one was a joint Opinion covering two notifications and seven were updated Opinions following updated notifications. We also issued seven non prior check Opinions, as well as two consultations on the need for prior checking.

83% of the risky processing operations we were notified about in 2017 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.

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 needs the detailed analysis of a prior check.

In 2017 the EDPS received six consultations on Prior Checking (Article 27.3), one of which was informal. We issued two formal consultative prior-checking Opinions.

We received 33 consultations on administrative measures (Articles 28.1 and 46 (d)), 12 of which were informal consultations. We issued 27 formal consultative Opinions and provided other advice at staff level.

Data minimisation

We received one complaint claiming that the Commission's Research Executive Agency (REA) breached the data minimisation principle. Data minimisation means restricting the collection of personal data to that which is strictly relevant and necessary to carry out a specific and pre-defined purpose. It aims to limit the amount of personal data that can be collected and processed.

The specific complaint related to the personal data required from individuals applying to be *external experts* through the online Grants Participants Portal. It argued that requesting a copy of the individual's identity card or passport, as well as their bank account number, before they performed any work for REA, was premature, and therefore excessive.

We investigated the case and ascertained that these documents were only requested from applicants after REA carried out a pre-selection process. We were therefore able to conclude that the collection of this personal data at this time was justified by the need to ensure the efficiency of the EU institutions and bodies; in this case, REA's grant allocation process.

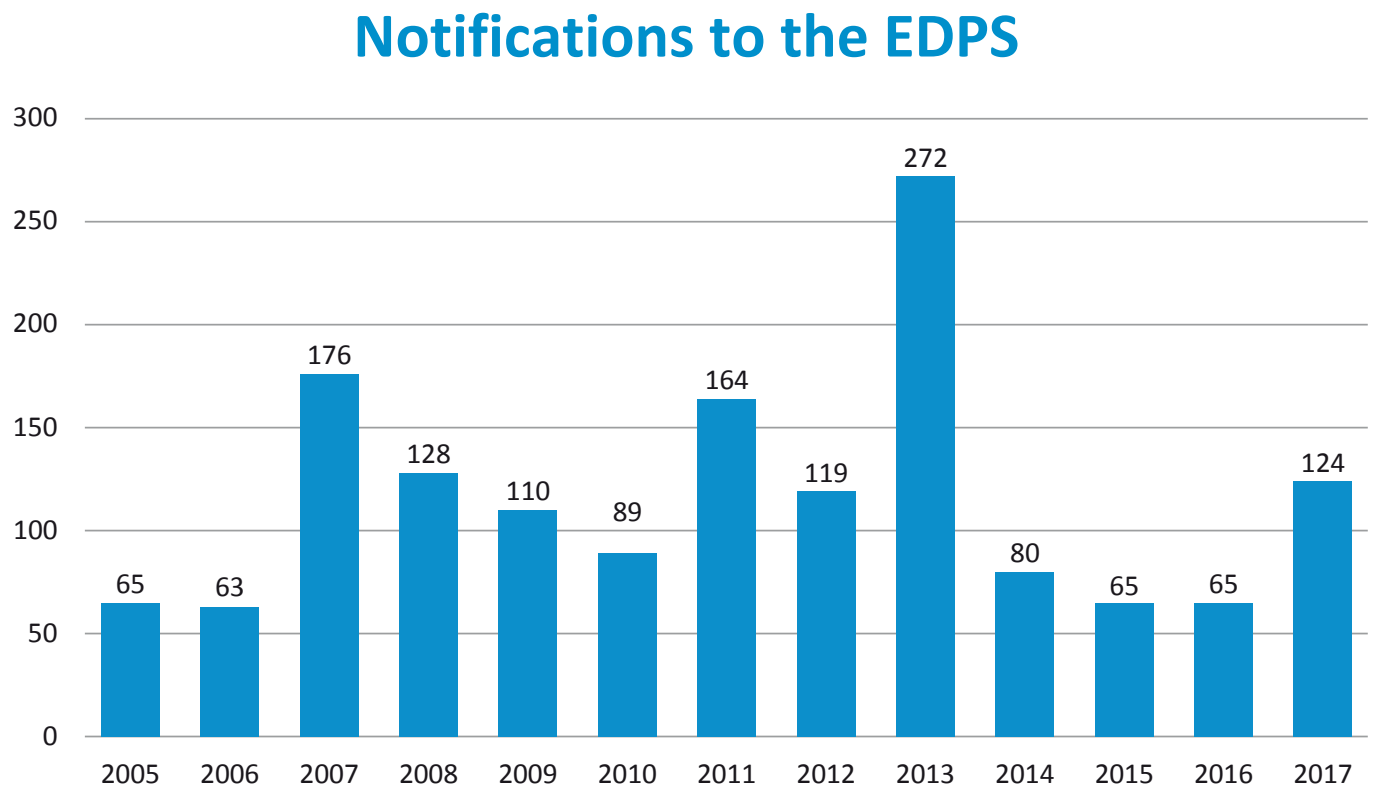


Fig. 5. Evolution of Notifications received by EDPS

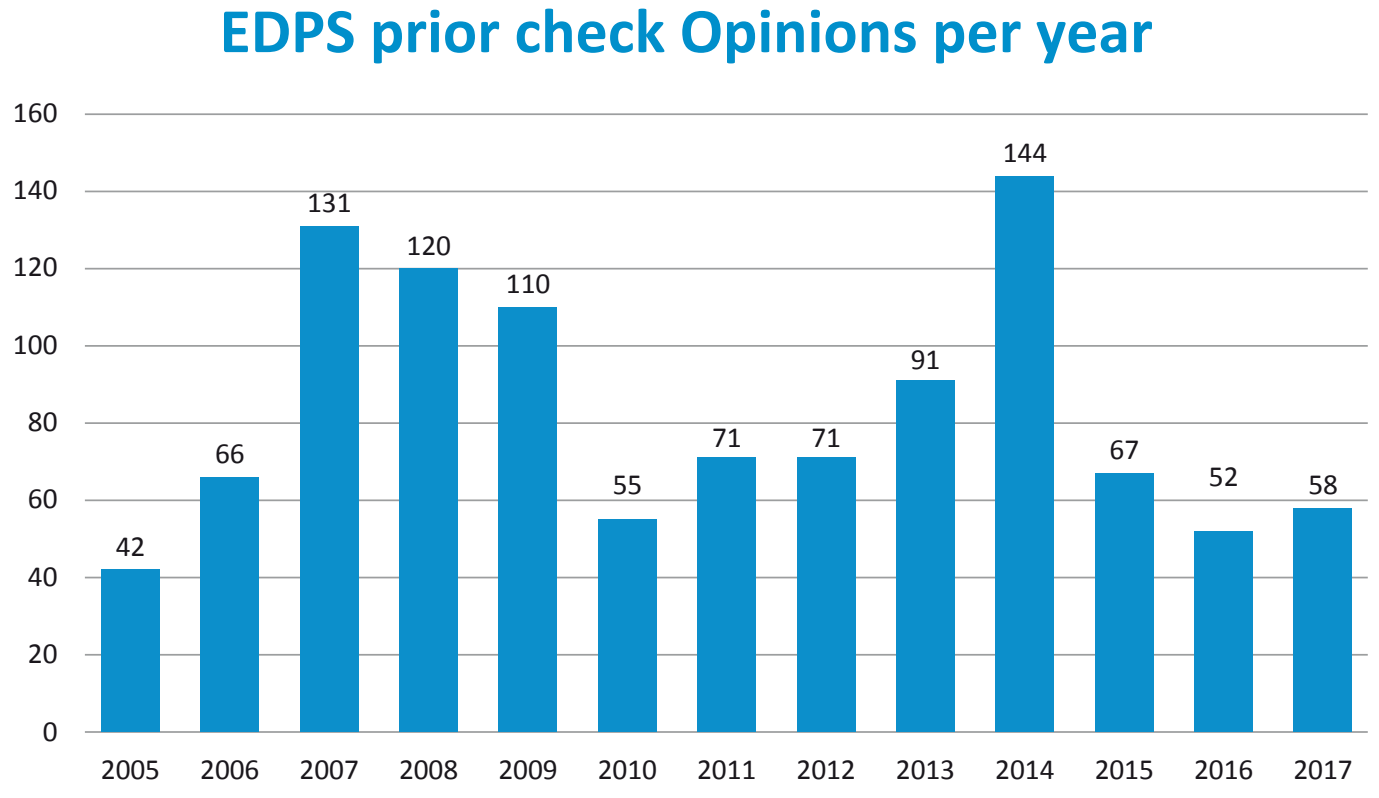


Fig. 6. Evolution of prior check Opinions issued by EDPS

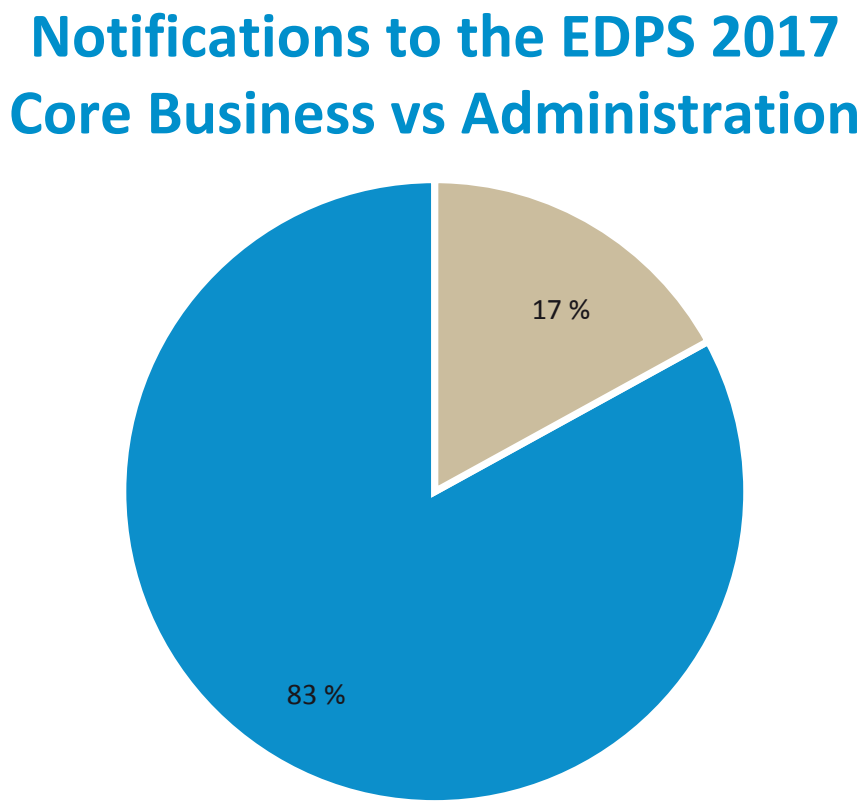


Fig. 7. Percentage split between Core Business (83%) and Administration (17%) activities in the Notifications received by EDPS

The case illustrates the chronological dimension of the data minimisation principle. In other words, it shows that the moment in time at which the data is collected must be taken into consideration when assessing compliance with the data minimisation principle. We asked REA to make some changes to the relevant privacy statement and the notification they had submitted to the DPO relating to this processing operation and, once we were satisfied with the action they had taken, we closed the case.

4.4.5 Catching up with the institutions: inspections and visits

Inspections and visits are two of several tools we use to monitor the EU institutions and ensure that they comply with the rules set out in Regulation 45/2001. Visits also help to raise awareness about data protection in the EU institutions, which is particularly important as we help them to prepare for the new rules.

In 2017 we carried out eight inspections and three visits. Our visits consisted of both compliance visits, which are used alongside inspections as an enforcement tool, and awareness-raising visits, which we have used as part of our efforts to help the EU institutions prepare for the revised Regulation, and the introduction of the accountability principle in particular.

The results of our inspections are shared directly with the institutions concerned. The EDPS then follows up in due course, to ensure that our recommendations have been put into practice. As part of our compliance visits, we work with the institution concerned to draw up a roadmap, designed to help them ensure compliance. These also involve a follow-up process.

We will continue to carry out visits and inspections as we move ever closer to the introduction of the new Regulation. Following the standards set out in our Strategy, the focus of our work will remain on ensuring

that the EU institutions have the right tools and knowledge to effectively move beyond a purely compliance-based approach, towards an approach based on accountability.

The EDPS is responsible for monitoring and ensuring the application of Regulation (EC) No 45/2001. Monitoring is primarily carried out in our biennial general surveys. The latest version of this general stock taking exercise is our 2017 Survey.

Inspections are one of several other 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 approach of the EDPS to inspections.

4.4.6 Advising the EU institutions

A digital Europe needs data protection

On 1 August 2017 we published an Opinion on the Commission's proposal for a Regulation establishing a single digital gateway and the once-only principle. Under the proposal, the exchange of evidence for specified cross-border procedures, such as a request for recognition of a diploma, would take place through a technical system. This system would allow national authorities to exchange data directly, but only at the explicit request of the individual concerned.

We welcomed the initiative as a necessary development in the modernisation of EU administrative services. As individuals would only be required to submit documents once and in one Member State, the availability, quality and accessibility of information across the EU would improve significantly. However, we also recommended that the Commission take into account some important data protection considerations as they continue to develop the once-only principle. This includes providing additional clarity on important data protection principles, such as the legal basis of the processing, purpose limitation and data minimisation.

The proposal also introduced amendments to the Internal Market Information System (IMI) Regulation. These clarify the coordinated supervision mechanism foreseen for IMI and would enable the new European Data Protection Board (EDPB) (see section 4.1.1) to benefit from the technical possibilities offered by IMI for information exchange under the GDPR.

@EU_EDPS

EU-wide once-only principle for lawful data exchange across EU borders needs data protection #singledigitalgateway - http://europa.eu/!by86Uu

An opportunity for stronger consumer and data protection

On 14 March 2017, at the specific request of the Council, we issued an Opinion on the Commission's Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. The proposal intends to extend consumer protection to digital content supplied to the consumer in exchange for money, but also in exchange for data.

We expressed support for the Commission's aim, which is to enhance consumer rights. However, our Opinion highlighted the risk of confusion for consumers and businesses relating to any new provisions in EU law that appear to treat personal information as a commodity, rather than a fundamental right. Under EU law, individuals are entitled to the same rights online as they are offline. This includes when consuming goods and services, whether they are supplied in exchange for money or not.

As the GDPR already legislates for the use of personal data in the digital economy, including the strict conditions under which the processing of personal data can take place in a contractual relationship, we urged the EU to avoid creating legal uncertainty by inadvertently interfering with these rules, and the rules to be covered in the future ePrivacy Regulation.

Developing the data-driven economy is essential for EU growth, but trust in that economy requires upholding fundamental rights. The proposal on digital content is an opportunity to ensure that future-oriented EU rules on data protection and consumer protection work in tandem in the interests of the individual.

Data protection on the farm

In December 2016, the Commission published a proposal for a Regulation on integrated farm statistics. The amendments proposed during the Council's discussions on the proposal, however, raised new issues regarding data protection, which were not present in the Commission's initial proposal. If included in the final text, the draft Regulation would become the first EU legislative instrument to provide for derogations from the rights of access and rectification, the right of restriction and the right to object to the processing of personal data for statistical purposes, in accordance with Article 89 of the GDPR.

With this in mind, the Council invited the EDPS to issue a formal Opinion on the proposed amendments, which we published on 20 November 2017. In the Opinion, we stressed that the rights of access and rectification are set out in the EU Charter and are considered essential components of the right to the protection of personal data. We therefore recommended that the Council re-assess the necessity of the proposed derogations. The fact that putting in place technical and organisational measures to provide access and other rights to individuals may require financial and human resources is, by itself, not a valid reason to derogate from the rights of individuals under the GDPR.

Unless the EU legislator is able to provide further justification of the need for these derogations, and tailor the scope of the provisions more narrowly, we recommended that they consider to what extent Article 11 of the GDPR, which refers to data processing that does not require identification, may help address the legitimate concerns of national statistical institutes.

Data protection and the fight against tax evasion

On 5 July 2016, the Commission proposed amendments to the Anti-Money Laundering (AML) Directive. The amendments would extend the scope of the Directive to tackle tax evasion and advocate a stricter approach to money laundering and terrorism financing. However, they could also have serious implications for data protection and privacy.

In our Opinion of 2 February 2017, we highlighted the areas in which the amendments constitute a cause for concern. Firstly, they suggest that personal data collected and processed under the current AML Directive, to counter money laundering and terrorism financing, might also be processed for other purposes, which are not clearly defined. This would contravene the principle of purpose limitation, which requires that personal data must only be collected and processed for a specific and pre-defined purpose. It also raises questions about the proportionality of the proposal, as it implies that the invasive personal data processing considered acceptable in the fight against money laundering and terrorism could be used to achieve other, undefined aims, for which the use of such methods might not be appropriate.

The amendments depart from the risk-based approach to data protection adopted in the current AML Directive and remove safeguards that help to establish proportionality. If implemented, they would pose significant and unnecessary risks to individual privacy and data protection. We therefore urged the Commission to re-think their position.

Privacy-friendly policymaking made easier

Almost all EU policy proposals now involve some form of personal data processing. Policymakers are also increasingly required to respond quickly to acute public security challenges and to keep up with developments related to the digital economy and international trade. The

need for help to ensure that each new proposal respects fundamental rights is therefore greater than ever.

Using an evidence-based approach, policymakers must be able to demonstrate that any planned limitation of the fundamental right to data protection and the right to private life is strictly necessary in order to achieve an objective of general interest or to protect the rights and freedoms of others. This also applies to the limitation of any other rights that might be affected by the processing of personal data.

@EU_EDPS

#EDPS publishes necessity toolkit as part of commitment to facilitating responsible & informed policymaking http://europa.eu/!Yu63VB

To assist policymakers in doing this, and as part of our commitment to facilitating responsible and informed policymaking, we published a Necessity Toolkit on 11 April 2017. It provides policymakers with a practical, step-by-step checklist, setting out the aspects to be considered when assessing the necessity of new legislation, and providing examples to illustrate each step. This is complemented by a legal analysis of the main concepts involved, such as the limitation of the right to the protection of personal data, the objective of general interest and the necessity and proportionality of an envisaged legislative measure.

4.4.7 New technologies

In 2016, the EDPS published a background document on the data protection and privacy implications of developments in Artificial Intelligence (AI) and Robotics. The paper was discussed at the 2016 International Conference of Data Protection and Privacy Commissioners in Marrakech, Morocco.

In cooperation with other DPAs, we have continued to work on the implications of AI for data protection and privacy throughout 2017, particularly within the International Working Group on Data Protection and Telecommunications (IWGDPT) (see section 4.5.2), and we hope to be able to contribute further to the debate in 2018

In addition, we have looked to widen our expertise, by examining the privacy implications of other new technologies, including connected glasses, Cooperative Intelligent Transport Systems (C-ITS) and the potentially disruptive application of AI and distributed ledger technologies, such as blockchain, to developments in the Financial Technology (FinTech) industry. Our work in these areas is ongoing, and we intend to provide relevant contributions on these topics during the course of 2018.

4.4.8 Privacy engineering gaining ground

With data protection by design set to become a legal obligation under the GDPR, interest in technological solutions for privacy is high. On 9 June 2017, the IPEN network, set up by the EDPS to promote privacy engineering and bridge the gap between legal and IT engineering approaches to data protection, organised a workshop to explore the practical consequences of the new obligations in depth.

The workshop, which took place in Vienna, aimed to highlight some new principles that could be used to ensure an increased level of protection for personal data. These included principles such as data minimisation, tracking protection, encryption and effective anonymisation.

Interest in privacy engineering techniques is also growing outside of Europe, particularly in the United States. On 10 November 2017, the Future of Privacy Forum (FPF) organised a multi-disciplinary Trans-Atlantic workshop in collaboration with IPEN, the Catholic University of Leuven and Carnegie-Mellon University. It focused on research and development needs in privacy engineering, particularly in relation to data protection by design and by default.

The workshop provided an excellent opportunity to focus on specific challenges associated with privacy engineering. These included exploring concepts such as *state of the art*, consent, de-identification, transparent and interpretable processing and deployment and development processes, and identifying open research and development tasks that will make the implementation of the GDPR successful.

4.4.9 The Digital Clearinghouse gets to work

The EDPS Strategy refers to the need to work across disciplinary boundaries to address policy issues with a privacy and data protection dimension. In this respect, consumer protection and data protection are natural partners, based on both the potential for imbalances in an economic transaction and the need for those who profit from the handling of personal information, in whatever way, to do so responsibly.

Regulatory bodies have the necessary tools to address questions relating to the concentration of market and informational power. Working together, enforcers of consumer and data protection law may be able to support antitrust authorities in their efforts by ensuring that mergers benefit the long-term interests of individuals and that dominant companies do not close down choice in the market or harm their customers, for example.

@EU_EDPS

.@Buttarelli_G #DigitalClearingHouse to bring together independent authorities to discuss & promote interests of individuals online #EDPD17

In response to their call to establish a space for dialogue, we launched the Digital Clearinghouse, which met for the first time on 29 May 2017. The meeting represented the culmination of several years of important discussions about how to respond to the digital challenge.

On 27 November 2017, a second meeting took place. Building on the discussions of the first meeting, we focused on several topics for which possible overlaps between domains or gaps in the regulation exist. These included the long-term impact of big technology sector mergers, the phenomenon of fake news, security considerations for the Internet of Things, harmful or unfair terms and conditions in online platforms and the generation of leads. The network will continue its work on these topics in 2018, with the possibility of extending our enquiries to consider the topics of unfair price discrimination and the liabilities of intermediaries.

Our efforts aim to bring together the various strands of work already underway in this area and to add value to existing projects.

4.4.10 Reinforcing cooperation on Fundamental Rights

On 30 March 2017, EDPS Giovanni Buttarelli and Director of the European Union Agency for Fundamental Rights (FRA) Michael O'Flaherty signed a memorandum of understanding on increasing cooperation between the two organisations. The document reflects the close and constructive relationship the EDPS and the FRA already share and marks a common intention to better exploit synergies in our work and roles.

@EU_EDPS

#EDPS & @EURightsAgency strengthen ties to improve #DataProtection #cooperation - Read blogpost by @Buttarelli_G https://t.co/FAPKQm2QBt

We are convinced that the rapport between data protection and privacy and other rights and freedoms under EU law is one of interdependence. Though the roles of our organisations are quite distinct, this memorandum of understanding should be seen as a statement of our determination to work in tandem to more effectively protect the rights and interests of the individual across all EU activities.

4.5. INTERNATIONAL AFFAIRS

The EDPS Strategy refers to the need to forge global partnerships. Our aim is to build a global social consensus on the principles relating to data protection and privacy. This includes working to mainstream data protection into international agreements, reinforcing cooperation with our EU partners in the Article 29 Working Party (WP29) to enable the EU to speak with one voice on the global stage and investing in relationships with international organisations and data protection networks.

It also includes working with both our international partners and the EU institutions to ensure that international data transfers can only take place in a manner that respects EU data protection laws. With the continued and rapid development of the digital economy and a shared international concern for public security, this has become a complex and hotly debated topic, and an important area of work for all EU data protection authorities (DPAs), including the EDPS.

In 2017, we increased our efforts on the international stage, improving our cooperation with international partners in an effort to develop and extend cross-border, coordinated approaches that protect the rights of individuals wherever they are in the world.

4.5.1 International data transfers

Ensuring data protection principles are safeguarded in trade agreements

One of the many signals that data protection is now truly part of mainstream public policy are the discussions taking place on the relationship between trade and data, including personal data.

Traditionally, data flows have not been considered a trade issue. However, with the rapid development of the digital economy, a new trend is beginning to emerge within the EU institutions. It relates to the idea that, in order to support the interests of EU businesses and allow them to be competitive in global markets, it is important to address restrictions to trade, known as digital protectionism.

This idea has led some to propose inserting specific clauses into the trade agreements negotiated by the European Commission, which would both ensure the *free flow of data* and prohibit *unjustified* data localisation restrictions put in place by trade partners.

The EDPS has repeatedly taken the position that data protection should not be a subject of trade negotiations. EDPS Giovanni Buttarelli reiterated this once more in an EDPS blogpost, published on 18 December 2017. We fully understand and support the trade interests of EU businesses and it is for this very reason that we support a genuine guarantee that EU data protection law will not be endangered by any trade agreement with a non-EU country.

References to the free flow of data are by nature ambiguous, because it is increasingly difficult, if not impossible, to distinguish personal data from other types of data. Moreover, introducing the clauses

proposed could lead to a potential conflict with EU data protection rules, including those relating to international data transfers.

By introducing rules on data localisation, the EU would run the risk of watering down existing EU data protection rules, or preventing the adoption of additional data protection rules in the future. Including data protection in the scope of trade agreement negotiations could also lead to the possibility of a non-EU country challenging EU data protection law, as a disguised restriction on the free flow of data.

To avoid uncertainties and to minimise unintended adverse consequences, personal data issues should be kept fully and explicitly out of the scope of the EU's trade agreements. Current and future EU data protection rules already provide us with the tools to ensure the free flow of data. The best way of addressing barriers to data flows is to make better use of these tools.

Privacy Shield under close scrutiny

On 30 May 2016, we issued an Opinion on the EU-US Privacy Shield draft adequacy decision, put forward to replace the invalidated Safe Harbour decision. The Privacy Shield has now been in place since 1 August 2016, and provides a framework allowing for the transfer of personal data from the EU to the US. In September 2017, the EDPS participated in the first EU-US Privacy Shield joint review. The outcome of this review was discussed at the WP29 Plenary in November 2017, and a report issued on 28 November 2017.

The WP29 report recognises the efforts made by the US authorities and the Commission to improve data protection through the implementation of the Privacy Shield. It also acknowledges that the Privacy Shield represents an improvement on the invalidated Safe Harbour decision. However, to date, the efforts made to implement the Privacy Shield are not sufficient and many of the concerns outlined in the 2016 EDPS Opinion remain valid. Specifically, the report notes the urgent need to appoint a permanent, independent Ombudsperson, as well as the remaining members of the Privacy Civil Liberties Oversight Board (PCLOB), and the need for further explanation on certain aspects of the rules of procedure relating to the Privacy Shield.

The WP29 report sets a deadline of 23 May 2018 for the Commission and the US authorities to address these immediate concerns. The remaining concerns outlined in the report should be addressed before the second joint review in autumn 2018, at the very latest. If these deadlines are not met, the WP29, of which the EDPS is a member, will take the appropriate action to achieve legal certainty. This could involve bringing the Privacy Shield adequacy decision to national courts, who have the power to refer the case to the EU Court of Justice for a preliminary ruling.

4.5.2 International cooperation

Supervising EFTA

On 4 October 2017, the EDPS signed a Memorandum of Understanding (MoU) with the EFTA Surveillance Authority (ESA), providing for EDPS supervision of the ESA, the authority responsible for monitoring the compliance of Iceland, Liechtenstein and Norway with the Agreement on the European Economic Area (EEA Agreement).

The agreement temporarily closes a legal vacuum. ESA has adopted data protection rules that are almost identical to those followed by the EU institutions, but lacks an external supervisory authority to monitor and enforce these rules. Working with the EDPS is therefore a temporary solution to this problem, which will also help to bring the EFTA states closer to the EU legal order, in line with the EEA Agreement. Additionally, a substantial part of the personal data processed by the ESA is exchanged with the Commission and, when processed by the Commission, is already subject to EDPS supervision.

We carefully analysed the legal basis for such an arrangement and found nothing to prohibit it. In fact, we strongly believe that this proactive and cooperative approach to international relations will prove to be of

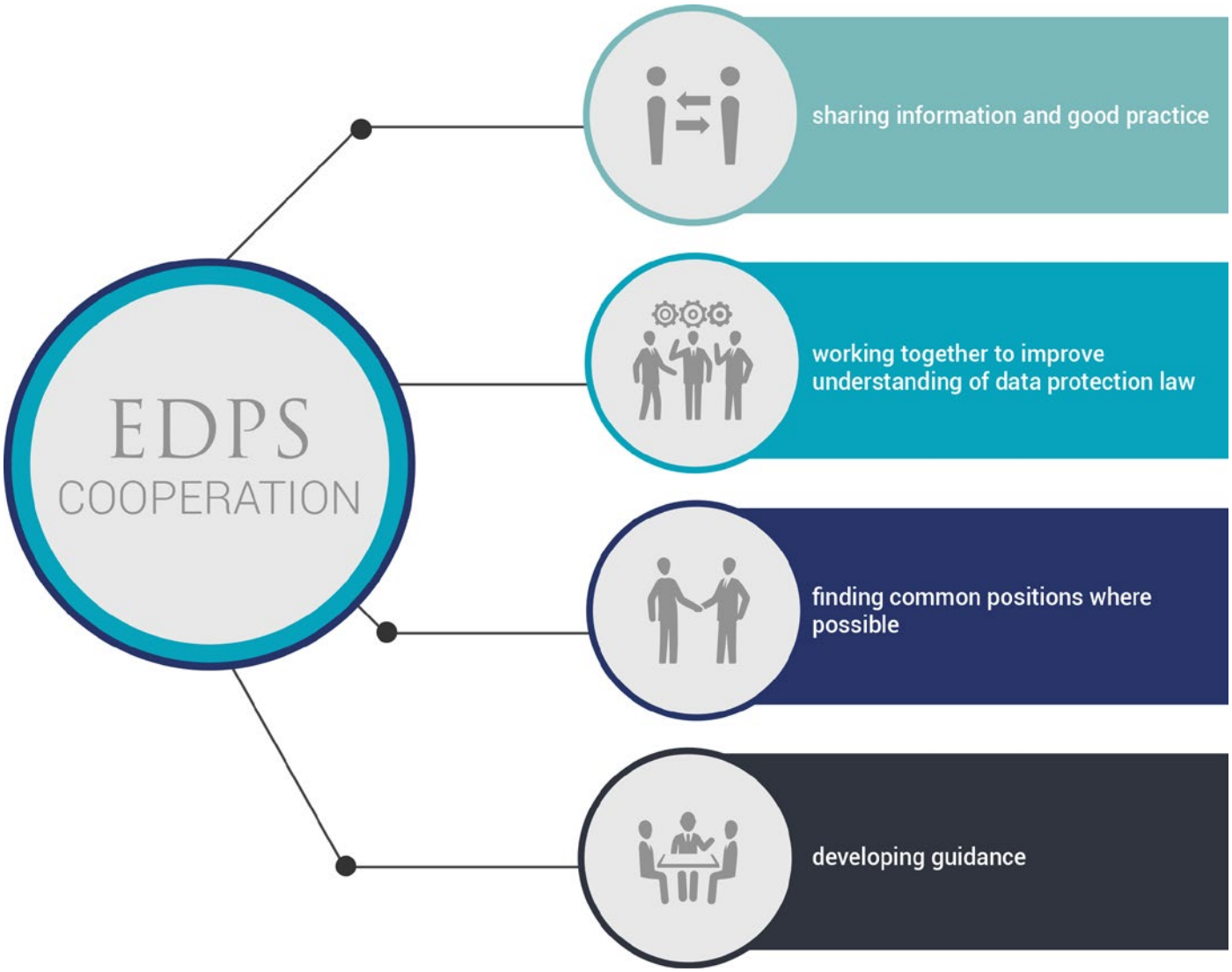
long-term benefit for data protection in Europe, and strongly supports our aim of further developing global partnerships in the interest of improving data protection, outlined in the EDPS Strategy.

Council of Europe

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

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

The Council of Europe is currently working on the modernisation of Convention 108, and in 2017 we continued to follow developments in this area. We also contributed to the T-PD's discussions on a draft recommendation on health-related data and on a practical guide on the use of personal data in the police sector, both of which the Council of Europe hopes to finalise in 2018.



The Organisation for Economic Cooperation and Development (OECD)

The EDPS also acts as an observer in the OECD Working Party on Security and Privacy in the Digital Economy (SPDE). This role involves providing advice to the European Commission where necessary, and providing comments on recommendations relating to data protection and privacy.

In May 2017, the Head of the EDPS Policy and Consultation Unit, Sophie Louveaux, gave a speech on national privacy and data protection strategies to the SPDE, which focused on topics such as the global recognition of data protection and privacy as human dignity rights, the global trend towards the development of data protection legislation, ethics and accountability.

The OECD also plays an active part in the workshops organised by the EDPS for international organisations (see section on International Organisations).

The International Conference

Hong Kong hosted the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC). Taking place from 25-29 September 2017, the focus of the conference was on connecting the West with the East. In particular, it addressed the different concepts and regulations used to define privacy across the world and the applicability of western models of data protection in Asia and elsewhere. The closed session of the conference looked to address government information sharing, with a specific focus on how to protect sensitive data, prevent discrimination and manage risk.

In addition to jointly hosting a side event on the common values that underpin privacy (see section 4.6.4), we contributed to three resolutions adopted at the conference, on connected and automated vehicles, collaboration with consumer protection authorities and internal enforcement cooperation. EDPS Giovanni Buttarelli also participated as a member of a panel on data protection and humanitarian action, as well as giving a speech at the closing ceremony.

In 2018, the international data protection community will meet in Brussels, where we will have the honour of hosting the 40th International Conference, alongside the Bulgarian data protection authority (see section 4.6.5).

The Spring Conference

Every spring, the data protection authorities from the EU Member States and the Council of Europe meet to share their experiences and exchange information on matters of common interest. This year's meeting took place in Limassol, Cyprus from 27-28 April 2017.

We actively contributed to the discussions, making significant contributions to resolutions on the rules and procedures of the conference and the modernisation of Convention 108. In addition, EDPS Giovanni Buttarelli chaired a panel on the dawn of new data protection regimes and participated as a speaker in a panel on the place of the Spring Conference in the new data protection regime.

International Organisations

As international organisations with offices in Europe are often exempt from national laws, many do not have a legal framework for data protection. To address this issue, we launched a series of workshops starting in 2005, aimed at supporting a constructive dialogue between international organisations on data protection and privacy. The sixth of these workshops on data protection within international organisations took place from 11-12 May 2017 in Geneva, and was organised in cooperation with the International Organisation for Migration.

Topics of discussion at the 2017 workshop included recent developments in data protection and privacy in international organisations, cloud computing, the processing of health-related data, the role of the data protection officer (DPO) and the impact of the General Data Protection Regulation (GDPR) on international data transfers to international organisations.

Following the positive feedback received from the organisations who took part, and considering the importance of maintaining and developing this dialogue, a seventh workshop is planned for 2018.

@EU_EDPS

70 members from 35 intl. organisations joining in Geneva to develop #DataProtection policies & #accountability in their worldwide practice

The Berlin Group

The International Working Group on Data Protection in Communications (IWGDPT) 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, and includes the EDPS.

Among other things, in 2017, the Group adopted working papers on biometrics in online authentication, e-learning platforms and international principles or instruments governing intelligence gathering. The EDPS participated in the work of the Group on these documents, and also contributed to working papers on connected vehicles and the processing of personal data under ICANN's internet domain registration rules.

Addressing ICANN

In collaboration with representatives from other international data protection organisations, including the UN Special Rapporteur and the Chair of the Committee of Convention 108, EDPS Giovanni Buttarelli took part in a series of high-level meetings and sessions from 13-15 March 2017, as part of the 58th meeting of the Internet Corporation for Assigned Names and Numbers (ICANN). We are also involved in related initiatives organised by the WP29 and the IWGDPT.

The meetings concerned ICANN rules and procedures regarding the WHOIS system, which provides for the retrieval of details about the owners of internet domains and IP addresses. The current rules and procedures provide for uncontrolled access to the personal data of individuals providing resources on the internet and force some service providers into conflict with EU data protection rules.

In all forums, we have urged ICANN to adjust its rules and procedures in order to ensure compliance with the GDPR before May 2018.

Regional and international data protection networks

The EDPS also cooperates with regional and international networks of data protection authorities as part of our efforts to forge and build on global partnerships. These networks include the Global Privacy Enforcement Network (GPEN), the Asia Pacific Privacy Authorities' (APPA) Forum, the French-speaking association of personal data protection authorities (AFAPDP) and the Ibero-American data protection network (RIPD).

Of particular note in 2017, EDPS Giovanni Buttarelli participated as a speaker at the 48th APPA Forum, which took place from 16-17 November 2017 in Vancouver, Canada.

4.6 DIGITAL ETHICS

4.6.1 The Ethics Advisory Group: Reflecting on Digital Ethics

Companies and governments are gaining increasing advantage from technological developments related to the Internet of Things, big data, robotics and Artificial Intelligence. Though these developments can bring many benefits for individuals and society, these

benefits depend on ensuring that our values, based on a common respect for the individual and human dignity, remain a core component of innovation.

In the EDPS Strategy 2015-2019, we set ourselves the goal of developing an ethical dimension to data protection. We wanted to explore whether regulating the digital world requires an ethical approach and the ways in which such an approach might be developed and implemented. We committed to establishing an independent advisory group on digital ethics, tasked with exploring the relationships between human rights, technology, markets and business models in the twenty-first century. Our aim was to start an international debate on the ethical dimension of data protection in the digital era.

In September 2015, we published an Opinion reaffirming our intention to set up this group. The Ethics Advisory Group (EAG) was then launched in early 2016, at the annual Conference of Computers, Privacy and Data Protection (CPDP).

The EAG, which consists of six individuals, all experts in their respective fields, is tasked with examining digital ethics from a variety of academic and professional perspectives. Their work has continued throughout 2017 and forms part of a broader discussion we have initiated on the digital environment and its ethical implications, taking place both in the EU and globally. This debate will culminate in the 2018 International Conference of Data Protection and Privacy Commissioners (ICDPPC). The Group's final report, providing an overview of their deliberations, will be used as one of the background documents for discussion at the conference.

4.6.2 Engaging in a multidisciplinary dialogue: the Data Driven Life Workshop

On 18 May 2017, the EDPS hosted a workshop on Data Driven Life. With the support of the EAG, the workshop aimed to further the discussion on digital ethics by exploring the positive and negative consequences of data-driven changes for society as a whole, and how these changes might affect our ability to pursue our own life choices.

This was the second workshop organised by the EDPS aimed at advancing the global debate on the ethical dimension of the digital revolution. The first took place in May 2016.

@EU_EDPS

.@Buttarelli_G keynote speech at #EDPS #DataDrivenLife workshop. #DigitalEthics is essential & one of #EDPS priorities for this mandate

Attended by academics and practitioners from the scientific and research communities, the Data Driven Life workshop focused on five areas in which data makes a big difference, with panels devoted to health and medical research, disaster response and risk management, the financial sector, democracy and smart cities.

The workshop proved a productive and informative forum for debate, providing valuable input for the work of the Group. Their conclusions will be integrated into the EAG report, to be published in early 2018.

4.6.3 Encouraging debate around the world

The digital revolution is fuelled by data, a significant proportion of which is personal data. As a result, data protection and privacy supervisory authorities find themselves with a significant role to play in the digital revolution. Tasked with trying to balance the tensions between data protection and digital innovation, the debate on ethics and how it might be used as a regulatory tool is of direct relevance to our work.

In the EDPS Strategy, we cite the importance of forging global partnerships to help data protection authorities to better respond to key data protection challenges. This means encouraging debate around the world and across disciplines. Though data protection and supervisory authorities might be best placed to understand the social impact of the digital revolution, we are unable to address the challenges it poses through the application of data protection alone.

As a multi-national and multi-disciplinary group, the work of the EAG plays an important part in this process. However, if we are to be successful in our efforts to develop an ethical dimension to data protection we need to go further. With this in mind, the EDPS, Assistant Supervisor and members of the EAG

secretariat attended several conferences throughout 2017 to present and promote the EDPS initiative on digital ethics. These included the annual CPDP Conference and the International Association of Privacy Professionals (IAPP) Conference, as well as events organised by Maastricht University and the Brussels Privacy Hub at the VUB University.

Our efforts will culminate in the 2018 International Conference, where the focus of the public session will be on facilitating an open and transparent conversation at global level, and across different disciplines, on digital ethics.

4.6.4 Thinking local, acting global: exploring common values that underpin privacy

Inspired by the theme of the 2017 International Conference in Hong Kong, which focused on connecting the West with the East, the UN special rapporteur on Privacy, the Digital Asia Hub and the EDPS jointly hosted a side event at the conference, focused on exploring what privacy means in different countries and cultures.

@EU_EDPS

Hong Kong Commissioner Wong welcoming #EDPS @digitalasiahub @UNHumanRights Thinking local, acting global: exploring common values #privacy

Aimed at data protection and privacy authorities and regulators, the event provided an interactive environment in which to explore the common values that underpin privacy and data protection. Participants were asked to discuss two questions in an attempt to determine whether enough common ground exists for the development of global standards of privacy:

- What does privacy mean to you in your country and why is it important?
- What are the values that underpin privacy in your country?

From our discussions, it was clear that though we generally agree on the values that underpin privacy and data protection, the relative importance we place on each of these values varies. For example, though freedom, dignity and fairness are considered common values, the relative importance assigned to each of these values varies from country to country.

At the 2018 International Conference we will look to develop this discussion further, in a similarly interactive environment.

4.6.5 The 2018 International Conference

The ICDPPC is an annual event attended by representatives from more than one hundred privacy and data protection authorities around the world. The EDPS and the Commission for Personal Data Protection of the Republic of Bulgaria have been given the honour of organising the conference in 2018.

Entitled *Debating Ethics: Dignity and Respect in Data Driven Life*, the conference will build on the work done by the EAG to explore how data and those who control it are influencing our values. It will take place in Brussels from 21-26 October 2018, with accompanying events in Bulgaria. A closed session, open to accredited members of the ICDPPC only, is expected to take place at the Palais d'Egmont in Brussels from 22-23 October 2018, followed by a public session from 24-25 October 2018, held at the European Parliament. The ICDPPC Executive Committee determines the topic of the closed session. The focus of the public session, however, is at the discretion of the hosts, and in 2018 it will focus on digital ethics.

Digital ethics is not a conventional theme for the ICDPPC, primarily because it is not a theme traditionally associated with data protection. However, as first-hand witnesses to the digital revolution, the EDPS believes that data protection regulators and

authorities should take a leading role in determining what our common values are and how we can protect them in the digital world. Though our conference programme is still in the development stage, we plan to focus on several questions, introduced in our conference video. These include:

- Do we need ethics in the digital world?
- Is technology still serving humankind?
- Should ethical considerations drive innovation?
- Is there an ethical dimension to data protection?

Our approach to the conference is also far from conventional. We aim to facilitate dialogue across a wide spectrum of groups and individuals from a range of disciplines. While the conference is already an important event for policymakers, civil society groups, academics and industry, we also want to reach out to other groups who might not traditionally associate their work with data protection. In another break with tradition, we plan to encourage participants to actively interact with one another and contribute their different perspectives to the discussion. An Advisory Committee will be appointed to provide input on our conference programme. More information on this committee and its members will be published on the conference website once the committee has been established.

@EU_EDPS

.@Buttarelli_G the theme of #icdppc2018 will be digital ethics #icdppc2017 closing ceremony

This is the first time that the conference will be organised by an EU institution together with a national supervisory authority. It is a unique opportunity for the EDPS, as the independent supervisory authority for the EU institutions, to continue playing a leading role in data protection, privacy and freedom of information across the world. It will also provide a timely follow-up to the Bulgarian presidency of the EU, which takes place in 2018.

4.6.6 Conference communication

The 2017 International Conference in Hong Kong provided the ideal opportunity for us to kick-start our communications campaign. We were able to promote the 2018 conference through a video, in which we introduced the topic and the questions we aim to explore. We also distributed an information leaflet about the conference.

In mid-2017, we invested resources in developing a logo for the 2018 International Conference. With the intention of raising awareness about the conference, we also encouraged designers from around the world to submit proposals. We will incorporate the logo into our promotional and conference materials, alongside some ideas from other proposals we received.

Work on the conference website is also underway and we aim to launch it in early 2018. To encourage participants to get involved in the wider online debate, we have also established the Twitter account @icdppc2018. An app, which will reflect and complement the website, is in the design phase. We plan to use it as a tool to encourage participants to interact fully with the conference programme and speakers.

5. Court Cases

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

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

Throughout 2017, we continued to closely follow all court cases relating to the protection of personal data. The rulings made on cases relating to data protection help us to interpret data protection law and to ensure that the fundamental right to privacy and data protection is fully respected.

5.1 EU-CANADA PNR UNDER FIRE

On 26 July 2017, the European Court of Justice issued an Opinion on the EU-Canada Passenger Name Record (PNR) agreement, signed by the EU and Canada in 2014. The Opinion, requested by the European Parliament in order to ascertain whether the agreement was in line with EU law, concluded that several provisions in the agreement were not compatible with EU fundamental rights, particularly those relating to respect for privacy and the protection of personal data. The Court therefore concluded that the European Parliament should not approve the PNR agreement in its current form.

At the request of the Court, the EDPS had intervened in the case on 5 April 2016. We also published a separate Opinion on PNR in 2015. The conclusions reached by the Court in the EU-Canada PNR case represent an important milestone for the EU, which is likely to affect other, similar agreements between the EU and non-EU countries, and this is something that we will continue to monitor in the future.

In the EU-Canada agreement, several of the provisions judged to interfere with the rights to privacy and data protection contravened the principle of necessity and failed to lay down clear and precise rules on the collection, transfer and processing of personal data. In particular, the Court cited provisions on the transfer, processing and retention of sensitive data, which failed to protect against the possibility of discrimination.

The Court held that the transfer and storage of PNR data for the purpose of entering Canada did not exceed the limits of necessity, as long as this data is only stored while the traveller remains in Canada. The use of any of this data during or after their stay would require new and justifiable circumstances, for which specific rules on the conditions of use and access would need to be developed. Retention of this data would be considered acceptable only in cases in which the travellers concerned present a risk relating to the fight against terrorism or serious transnational crime.

In order to be compatible with EU law, the agreement must, among other things, provide more clarity on the types of PNR data that can be transferred. Moreover, the right for air passengers to be notified if their PNR data is processed during their stay in Canada or after their departure should also be established, as well as an independent supervisory body to oversee the use of PNR data in Canada.

@EU_EDPS

#CJEU decision on EU-Canada #PNR in line with 2013 #EDPS opinion - Read more https://t.co/mtp2HLd76U

6. Transparency and Access to Documents

As an EU institution and according to our Rules of Procedure, the EDPS is subject to Regulation 1049/2001, on public access to documents. In 2017, the number of public access requests received for documents held by the EDPS decreased slightly, from 13 requests in 2016 to 11 requests in 2017.

In 2017, the EDPS launched a new website, designed to make it easier for users to follow the activities of the EDPS and to find the information they need. We also publish the agendas and meetings attended by the EDPS and the Assistant Supervisor on our website, in an effort to increase transparency. In 2018, in addition to responding to requests for public access to documents, we will continue to implement measures designed to increase the transparency of our work.

7. The Secretariat

7.1 INFORMATION AND COMMUNICATION

With new technologies emerging every day, general public concern about how our data is used and collected, and an interest in how it can best be protected, is increasing. As the role and responsibilities of the EDPS continue to grow, our ability to communicate about the work we are doing is more important than ever.

Unsurprisingly, the activities of the EDPS Information and Communication team have both diversified and intensified over the course of 2017. The launch of a new EDPS website in early 2017, followed by a new-look Newsletter in the summer, marked the end of a successful attempt at rebranding and updating the image of the institution, in line with the ambitions laid out in our Strategy 2015-2019. Meanwhile, work on developing websites and communication tools for the European Data Protection Board (EDPB) and the 2018 International Conference (see section 4.6.6), also got underway. With deadlines for both events approaching, the importance of our communications activities will only continue to increase as we move into 2018.

7.1.1 Online media

Website

In March 2017 we launched the new EDPS website. The launch marked the culmination of several months of work, involving the design of a new layout, the migration of content from the old website to the new one and the transition to a new content management system (CMS).

The website features a new layout, designed to be more accessible and transparent. It provides easy access to EDPS work, which is organised by topics, and to social media, through a Twitter wall. The homepage features new content such as the history of the new General Data Protection Regulation (GDPR) and our latest blogposts and videos. We have also introduced a powerful new search engine, making it easier for users to find the information they need. The website is mobile oriented and therefore easy to access using any device.

Unsurprisingly, the number of visitors to the website in 2017 decreased in comparison to 2016. This is because the figures for 2016 were unusually high, due to our work on the transition to the new website. Moreover, the statistics for 2017 only take into account the number of visitors to the website since its launch in March 2017. However, the feedback we received after the launch of the new website was very positive and the number of visitors is sufficiently high for us to conclude that it is an increasingly valuable online resource for those interested in our work and in data protection in general.

Social Media

The importance of social media as a communications tool for the EDPS cannot be underestimated. With our presence on social media now well established, we are able to easily reach a global audience using a variety of channels.

The EDPS Twitter account (@EU_EDPS) is our most influential social media tool. Our number of followers increased significantly once again, in 2017, increasing our global reach. The number of times we tweeted remained consistent with the figures from 2016, with our principal aim being to ensure that all our tweets are both relevant and informative for those who engage with us.

The EDPS presence on LinkedIn also continues to grow. The number of users who follow the EDPS has increased significantly and it remains an excellent platform for promoting EDPS activities, events, documents and news.

In 2017, the EDPS published a record 36 videos on YouTube, 22 of which were also published on our website. There was also a corresponding increase in

the number of followers on our YouTube channel. 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

The EDPS blog was launched in April 2016 and is now an integral part of our communication activities. Blogposts are published on a regular basis, with the aim of providing a more detailed insight into the work of the EDPS, and the Supervisors in particular. The blog can be easily found on the homepage of the EDPS website.

We published 16 blogposts in 2017 on a range of subjects, including our work with Data Protection Officers (DPOs), Digital Ethics, communications privacy and the Digital Clearinghouse. We also distributed some of the blogposts to our network of journalists and other interested parties, and several received media attention.

7.1.2 Events and publications

Data Protection Day 2017

Data Protection Day takes place annually on 28 January. In 2017, we celebrated the eleventh edition by organising a lunch conference on the Internet of Things for trainees from the EU institutions. The conference was also live-streamed on our website and debate was encouraged online through a dedicated twitter hashtag. The event was an excellent opportunity to communicate directly with young people and address their questions on a topic of increasing relevance to our everyday lives.

The annual Computers, Privacy and Data Protection (CPDP) conference, attended by data protection professionals from around the world, took place in the days leading up to Data Protection Day 2017 and, once again, the EDPS played an active part. EDPS experts gave a range of presentations at the three-day conference, which focused on the theme of Artificial Intelligence. The EDPS also hosted a panel discussion on Ethics in the Digital Era. Members of the Ethics Advisory Group (EAG) returned to CPDP, where we launched the group a year earlier, to discuss their work to date (see section 4.6.3). The event was an excellent opportunity to explore digital ethics in an international environment, and therefore further our aims for the group in line with the EDPS Strategy.

@EU_EDPS

28 January 2017 - #EDPS celebrates #DataProtectionDay!

EU Open Day 2017

On Saturday 6 May 2017 we participated in the annual Open Day of the EU institutions and bodies in Brussels. The event provides us with an opportunity to increase general public awareness of data protection and the role of the EDPS.

In a break with previous years, in 2017 the EDPS stand moved to the European Commission's Berlaymont building. Throughout the day, EDPS staff were on hand to answer questions on privacy rights and the protection of personal information. Visitors were also able to test out our facial detection software, which determined their sex, age and mood.

The day was a great success, with a record number of people participating in the EDPS quiz and significant interest in the activities on offer and the work of the EDPS. With the profile of data protection and privacy only set to increase over the coming years, we are already looking forward to welcoming visitors back to our stand in 2018.

Newsletter

Following the successful launch of our new website in March 2017, the EDPS Newsletter also underwent a makeover. By switching to a new, online, mobile-friendly format, our intention was to make the Newsletter more accessible and user-friendly, regardless of the device used to read it.

The Newsletter is distributed to our Newsletter mailing list and can be found on our website. Though the content remains the same, we now publish the Newsletter on a more frequent basis, allowing us to keep our readers better informed about our activities and other developments in data protection.

The first edition of the new-look Newsletter was published in June 2017 and, in total, we published six editions of the Newsletter in 2017. Our mailing list also continues to grow, demonstrating the importance and relevance of the Newsletter as a communication tool.

7.1.3 External relations

Media relations

In 2017, we issued 12 press releases and statements. The decrease in figures in comparison to 2016 comes as a result of our increased use of the EDPS blog and our social media channels, both of which have proved effective in generating media coverage. We published all press releases on our website and distributed them to our network of journalists and other interested parties. They were also published on the EU Newsroom website.

In addition to this, we received 22 written media enquiries and the EDPS and Assistant EDPS gave 33 direct interviews to European and international journalists.

Using social media alongside our press activities, in addition to the EDPS blog, has helped us to strengthen our media strategy and achieve maximum impact for our most influential activities. In particular, we received significant press coverage for EDPS work on the Privacy Shield, ePrivacy and the 2018 International Conference. Media coverage has been particularly notable in Italy and Poland, the countries of origin of the EDPS and the Assistant Supervisor respectively.

Study visits

We welcomed 12 groups to the EDPS for study visits in 2017. The majority of these came from European universities, although we also welcomed legal and privacy professionals and colleagues from other EU institutions. Study visits enable us to interact directly with young people and influential groups and to raise awareness about the importance of data protection and the work of the EDPS.

Information requests

We witnessed another significant increase in the number of public information requests received by the EDPS in 2017. Many of these requests relate to matters over which the EDPS has no competence, while others request information on privacy matters or assistance in dealing with problems related to the protection of personal data.

It is safe to assume that the increase in requests is primarily due to the introduction of the GDPR and the need to ensure compliance with these new rules. Combined with the increased visibility of the EDPS, this means more and more people are turning to us for help. We reply to all requests with information relevant to the individual enquiry, referring the requester to the relevant service if their request falls outside our competence.

7.1.4 Preparations for the European Data Protection Board

Website

The transition to a new EDPS website served as the starting point for the creation of the EDPB website, which we will launch in May 2018. In contrast to the previous CMS used to host the EDPS website, EC Drupal provides us with the opportunity to reuse existing features to create other websites with similar specifications. Work on the new website is now well underway.

Logo and visual identity

In collaboration with the EDPB Task Force, in which the 2017 Chair and Vice-Chairs of the Article 29 Working Party (WP29) are represented, we came up with some designs for an EDPB logo. From these designs, a logo was then selected by the WP29 members and a corporate identity developed specifying the way in which the logo can be used.

7.2 ADMINISTRATION, BUDGET AND STAFF

The Human Resources, Budget and Administration (HRBA) Unit provides support to the Management Board and operational teams at the EDPS, helping them to achieve the goals set out in the EDPS Strategy 2015-2019. In addition to performing traditional HR activities, the Unit is also responsible for carefully managing the institution's small budget and implementing new policies to ensure that working life at the EDPS runs smoothly. For example, in 2017 we introduced an HR Forward Planning tool, continued our work on the Data Protection Accountability project, and put frameworks in place to promote equal opportunities and diversity.

7.2.1 Budget and finance

Budget

In 2017, the EDPS was allocated a budget of EUR 11 324 735. This represents an increase of 20.9% compared to the 2016 budget. The 2017 budget was heavily influenced by two major legislative changes, the new General Data Protection Regulation (GDPR) (see section 4.1) and the Europol Regulation (see section 4.2), both of which require increased human and financial resources.

The budget of the EDPS is entirely administrative and is so small that salaries (remunerations and allowances) amount to around 64.5% of the whole budget. As a result, the incorporation of new posts has a significant impact on the budget. The Budget Authority granted the EDPS six new full-time positions to carry out tasks under the new Europol Regulation, and two and a half for the setting up of the new European Data Protection Board (EDPB).

We expect the budget implementation rate for 2017 to be around 90%. This is lower than hoped, due to two major factors:

- The proportion of the budget which accounts for salaries makes it very difficult to get any closer to a 100% implementation rate. This is because a moderate turnover of staff, or even a few members of staff taking personal or parental leave, has a disproportionately negative effect on the overall implementation rate of the budget.

- In 2014, Title 3 of the EDPS budget was issued to cover the budgetary needs of the EDPB. Resources have been progressively allocated to this Title since 2015, to prepare for the setting up of the Board, but our budget estimations were often done with imperfect information and some preparatory activities have occurred at a different pace than originally predicted. These difficulties are likely to persist for the next few years, until the EDPB becomes a fully mature organisation.

Finance

For the sixth consecutive year, the Statement of Assurance of the European Court of Auditors concerning the financial year 2016 (DAS 2016) did not contain any observations on the reliability of our annual accounts.

Procurement

In 2017, we launched a call for tender relating to promotional items. This was awarded to the value of 60.000 EUR.

Some major projects and contracts were also concluded through inter-institutional Framework Contracts (FWC). These included:

- **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 reviewed our approach to procurement activities in a document entitled *Procurement Professionalisation*. It includes some recommendations that we plan to implement over the course of 2018. It has two main objectives:

- the appointment of a single Operational Initiating Agent in each of the EDPS' operational units and sectors. These individuals will receive proper training on negotiated procedures for low and middle value contracts;

- the move to a completely paperless procedure, based on an electronic workflow.

7.2.2 Human Resources

Career guidance

In 2017, we launched a major project aimed at providing career guidance to all EDPS staff. The EDPS is currently undergoing internal changes associated with the creation of the EDPB and internal reorganisation. The exercise assisted in the identification of staff members interested in working for the EDPB, as well as helping staff to think about their career progression.

Confidential career guidance sessions were proposed to all members of staff apart from managers, and took place on a voluntary basis throughout autumn 2017. The objective of these interviews was to listen to the wishes and expectations of individual staff members and provide them with information, if relevant, about their career opportunities. Follow-up meetings and actions were organised on a case by case basis.

Anonymous interim and final reports on the exercise were presented to the EDPS management, outlining some conclusions and recommendations.

Staff Retention

Our success as an organisation depends on our staff: their talent, creativity, knowledge and commitment. We have always endeavoured to attract and recruit staff members with the necessary competencies, skills and knowledge to achieve our strategic goals, bearing in mind that the impact of early departures for a small institution like ours is much more costly and detrimental than for bigger EU institutions.

In 2017, we began to implement our new staff retention policy, adopted in 2016. This also involved reviewing some policies, such as the teleworking decision, in order to enlarge the scope and offer more flexible working conditions to staff. In addition, line managers and top managers were encouraged and reminded to keep their staff motivated by giving recognition and constructive feedback, while internal communication between HRBA and other teams also improved, due to initiatives such as HRBA breakfasts, which encouraged informal communication between the teams.

We also endeavoured to improve training and career development by introducing new learning and development activities, such as in-house training sessions and personal career guidance interviews.

For all new staff members, our aim is to ensure that, from day one, they feel as though they are an integral part of the EDPS team.

Security decisions

In 2017, we continued our work on developing a new Security Package for the EDPS. The package consists of a new Decision on Security and the review of the Decision on the Protection of European Union Classified Information (EUCI), which will be assessed in May 2018 to ensure that the approaches of both the EDPS and the new EDPB are consistent.

We reviewed our security policies in line with the benchmark set by other EU institutions, but particularly the Commission's rules on security, adopted in 2015. As the EDPS has already taken over the supervision of Europol, and may also take on a similar role for Eurojust and the European Public Prosecutor's Office in the future, it is essential that we are able to guarantee a level of security at least equivalent to the level in place in these agencies.

The Security Decision concerns the security of persons, assets and information. It also defines the organisational aspects related to security in the EDPS. It is based on the classic principles related to 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. It also describes the tasks of all the actors involved, such as the Security Committee, the IT Steering committee, the Local Security Officer (LSO), the Local Information Security Officer (LISO) and the Data Protection Officer (DPO).

The reviewed EDPS Decision on the Protection of EUCI aims to fine-tune the previous Decision, adopted in 2014, to bring it in line with the recommendations made by the European Commission after a security inspection carried out in July 2012. The Decision

ensures equivalence of protection with EU institutions on the handling of EUCI. This is particularly important as our work with Europol is likely to result in the processing of an increased amount of classified information. In terms of physical security, we have introduced updates to the Decision relating to the so-called Secure Areas. This is imperative as the EDPS does not have its own Secure Area and relies on those of the Commission.

The Business Continuity Plan (BCP)

A revision of the EDPS BCP is currently underway and is due to be completed by spring 2018. Our aim is to bring the policy more in line with the current role and internal organisation of the EDPS.

HR Forward Planning

In autumn 2017 we launched a new strategic tool known as the HR Forward Planning (HRFP) tool. These kinds of tools help managers to determine how to fill the gap between current resources and future needs, in accordance with the organisation's strategy.

Our Internal Auditor recommended that the HR team develop and implement an HRFP tool to support the Supervisors in the implementation of the EDPS Strategy. The EDPS HRFP has an annual cycle and involves several steps, used to estimate the resources and HR policies required to achieve our business needs. This tool is particularly helpful in the development and planning of selection procedures and learning and development actions, as well as in the development and update of HR policies or budgetary transfers.

Equal opportunities and diversity

If we are to make the most of the talent, creativity, ambition and commitment of those who work for the EDPS, we must ensure the effective and fair management of employees and the environment in which they work.

In 2017, we continued the EDPS Head of Activity Development Programme. Through a series of workshops, the programme aimed to develop cooperation and communication between participants, as well as to create a network and enhance the visibility of its female participants. Individual coaching sessions were also organised to follow up.

A new telework decision, aimed at improving working flexibility at the EDPS, was signed in July 2017 and two training courses, on *preserving respect and dignity at work* and *managing teleworkers and people at distance*, were organised to encourage a culture of respect within the institution and to provide guidance on how to implement the new telework decision. Training sessions on emotional intelligence also took place.

To better accommodate people with disabilities, we also altered our job application form and privacy statement. This will help our institution to become a welcoming work environment for a diverse workforce.

Data Protection Accountability

Throughout 2017, the HRBA unit continued to use the data protection accountability tool put in place in 2016, and to update the associated questionnaire. The tool helps us to ensure the accountability of the HRBA unit: our willingness to ensure compliance with data protection obligations and to produce documentation proving that this is the case.

In collaboration with colleagues from the EDPS Supervision and Enforcement Unit, we organised a workshop to raise awareness about the tool within the HRBA Unit and to share our experiences using the tool. Our Supervision and Enforcement colleagues provided us with some recommendations relating to the use of the tool, which were added to the relevant internal action plan.

Preparing for the EDPB

The EDPS is responsible for ensuring that the EDPB receives adequate human and financial resources from the budgetary authority and is administratively prepared to perform its new role (see section 4.1.1).

In November 2017, a sector in charge of EDPB matters was established. Several EDPS staff members were transferred to this new sector, charged with carrying out the necessary preparatory tasks required before the EDPB Secretariat assumes its role in May 2018.

Reporting lines will be clarified in the Memorandum of Understanding and Rules of Procedure to be signed between the EDPS and the EDPB.

For administrative matters, HRBA and the Information and Communication Sector will serve both the EDPB and the EDPS. From May 2018, the EDPS Director will remain the appointing authority (AIPN) for the EDPB Secretariat, but the Secretariat staff will work under the instructions of the EDPB Chair only.

We have also set up an ambitious recruitment plan for the first half of 2018, using the HRFP.

Increasing the visibility of our institution

On 9 November 2017, we took part in the European Commission's Career Day for the first time. Two representatives from the EDPS gave a presentation focused on career opportunities at the EDPS, and the advantages of working for our institution.

We will request to take part in all future career days organised by the European Commission, not only in terms of a dedicated presentation slot, but also through requesting an EDPS stand, to improve EDPS visibility further.

8. The Data Protection Officer at the EDPS

8.1 THE DPO AT THE EDPS

It is fair and correct to assume that the average level of awareness of data protection requirements among staff members at the EDPS is high. However, the existence of a Data Protection Officer (DPO) is just as important in the EDPS as it is in the other EU institutions and bodies. The presence of a staff member explicitly tasked with monitoring and facilitating the protection of personal data is essential in order to transform even a high level of awareness into action.

In anticipation of the increased workload associated with the introduction of new data protection rules for the EU institutions (see section 4.1.3), the DPO office at the EDPS has been reinforced. In October 2017 we appointed a part-time Assistant DPO. He will support the DPO in ensuring that the EDPS sets an example that other institutions can follow.

8.2 PREPARING FOR THE NEW REGULATION: THE DATA PROTECTION ACCOUNTABILITY PROJECT

In 2016 we launched a personal data accountability project, aimed at improving accountability at the EDPS (see section 7.2.2). Our intention was to lead by example, as required by the EDPS Strategy, in our implementation of data protection requirements and principles, as well as to increase our credibility and knowledge as the authority responsible for ensuring data protection compliance in the EU institutions. The EDPS DPO managed the project and all EDPS units and sectors contributed to the planning and execution phases. The resulting tool relies on an evidence-based questionnaire, which was completed by the relevant members of staff in 2016.

In 2017, we assessed the results of the questionnaire, which allowed us to plan and execute a number of activities aimed at improving data protection practice at the EDPS. We also reviewed the questionnaire itself, to ensure that it accurately reflects the proposal for the reform of Regulation 45/2001 (see section 4.1.2). This was also necessary in order to ensure that the exercise provides a relevant example for the other EU institutions and bodies, which we can use as part of our activities to prepare the institutions for the new Regulation. Following this update, one institution has already made the decision to use our questionnaire as part of their own accountability strategy.

At the end of 2017, EDPS staff members completed the questionnaire once more. In 2018, we will incorporate the results into the EDPS data protection action plan, as we did in 2017.

We have also drawn up a plan to ensure that the EDPS remains compliant and effectively accountable in relation to the new rules. The actions specified in the plan range from reviewing processing operations and the way they are documented to creating new procedures, including those needed to handle personal data breaches, to perform Data Protection Impact Assessments (DPIAs) and to manage enquiries or requests from individuals about their own data.

8.3 ADVISING THE INSTITUTION AND IMPROVING THE LEVEL OF PROTECTION

As in past years, in 2017 the DPO provided advice on a number of new processing operations and internal policies carried out at the EDPS. They included:

- improvements to the EDPS website and the development of a new website and app for the 2018 International Conference of Data Protection and Privacy Commissioners;
- some aspects of the EDPS Security Decision and Information Security Policy;

- staff recruitment, underperformance and anti-harassment procedures;
- the EDPS Case Management System;
- meetings and events organised by the EDPS.

8.4 THE REGISTER OF PROCESSING OPERATIONS AND NOTIFICATIONS

Under Article 26 of the Regulation, the DPO must keep a register of all notifications relating to the processing of personal data carried out by the institution. In 2017, two new notifications were published and three were updated. The Register of all notifications is available for public consultation on our website.

We also notified the EDPS, as our supervisory authority, of three planned data processing operations. We have received recommendations relating to one of these notifications and are working to implement them.

8.5 DEALING WITH ENQUIRIES

In 2017 we received eight requests from individuals for access to their personal data, processed by the EDPS. Some of these requests were also requests for erasure of this data. The number of requests received by the EDPS is increasing year on year.

In general, the DPO acts as a coordinator and supervisor for the respective replies, the content of which is prepared by the relevant member of staff.

8.6 PROVIDING INFORMATION AND RAISING AWARENESS

The DPO meets all new staff and trainees personally for a short welcome meeting and data protection induction course. Twelve such meetings took place in 2017. Each meeting is customised to meet the needs and role of the staff members concerned. Topics may include:

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

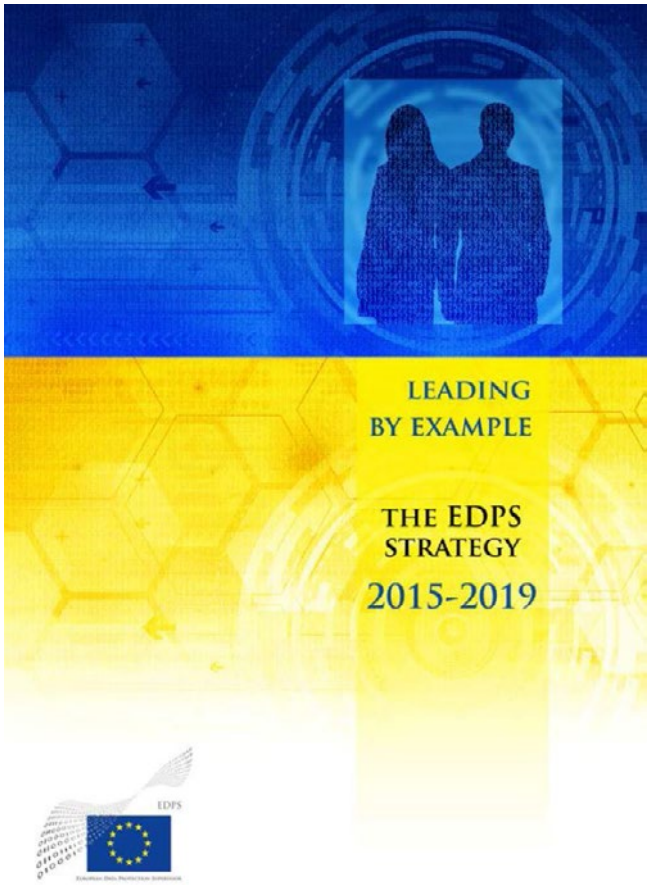
Internal EDPS coordination and information meetings and the use of the DPO sections on the EDPS Intranet and website, which are regularly updated, also represent opportunities to reach out to staff members and external stakeholders.

In addition, the meetings of the DPO network (see section 4.4.1), which took place in Tallinn and London in 2017, provide the EDPS DPO with an excellent opportunity to discuss common issues and share experiences and best practices with colleagues from the other EU institutions.

9. The mid-term Strategic Review

To ensure our work remains on track, we committed to carrying out a mid-term review of the EDPS Strategy in consultation with our stakeholders, and reporting on the results of this review in our 2017 Annual Report.

An external consultant performed the review, carrying out interviews of fifteen internal and external stakeholders in September and October 2017, using a questionnaire (see figure 8). External stakeholders included representatives of European national data protection authorities (DPAs), members of the data protection officer (DPO) community, representatives from the EU institutions involved in policy and data control, members of the technology community and representatives from NGOs dealing with personal data and the protection of human rights. On 30 November 2017, during an EDPS Management Away Day, the consultant reported on the feedback received. Our discussions resulted in the conclusions below.



9.1 EVALUATING OUR ACHIEVEMENTS

The approach adopted in the EDPS Strategy was considered very successful, with one external stakeholder commenting that *the new supervisors have splendidly taken over the baton from the previous team*. The new Supervisors brought about a vast transformation in the vision, mission and strategy of the organisation, with the aim of driving it into a position of global leadership and visibility.

Those interviewed appreciated the constructive, pragmatic and client-oriented approach adopted by the EDPS. External stakeholders took the view that the EDPS should continue to do what it does well: advise, provide expert analysis and stay in contact with the EU institutions, while ensuring it is not perceived as *obstructionist*. The Strategy is effectively transforming the EDPS from a centre of excellence for study and legal analysis into an *international centre of gravity* in the world of data protection.

The results of the review allowed us to conclude that there is no need for fundamental changes to the mission or the strategic objectives outlined in the Strategy. All of them remain relevant. There have been no significant, unexpected developments in data protection since the publication of the Strategy in early 2015 and the institution is where we expected it to be at this point in the mandate. We were also able to predict a number of developments, such as increasing interest in the ethical dimension of the processing of personal data and certain decisions made by the EU Court of Justice (CJEU).

9.2 ENSURING AN EFFECTIVE APPROACH TO THE SECOND HALF OF OUR MANDATE

To account for the impact of external factors that could not have been predicted in 2015, such as Brexit, the new US administration and terrorist attacks, we decided that some limited adjustments to the Strategy might be appropriate.

We also accepted that the workload relating to some tasks, such as Europol Supervision (see section 4.2) and the setting up of the new European Data Protection

Board (EDPB) (see section 4.1.1), might have been underestimated. Although our cooperation with stakeholders was generally considered satisfactory, some of those interviewed expressed concerns about future relations with the EDPB and the need for the EDPS to be able to supervise all EU bodies, including those in the areas of Justice and Home Affairs.

Some internal stakeholders expressed the view that the path between Strategy definition and Strategy execution is not always sufficiently clear. While the way in which the EDPS interacts with the outside world has changed significantly, the way the institution works internally has not changed so much. Some limited organisational changes might therefore be appropriate, to ensure that the organisation is functioning as well as possible by the end of the mandate. Particularly important is to improve internal communication between the EDPS and Assistant Supervisor and the rest of the organisation, as well as to better prioritise tasks. At the request of the EDPS and Assistant Supervisor, the Acting Director at the EDPS will launch discussions with managers and the Staff Committee and submit an action plan to the Management Board. This plan will address smarter ways of working, increased delegation of tasks and additional measures aimed at better managing the workload at the EDPS.

Both external and internal stakeholders agreed that the organisation is seriously understaffed, both in number and in some fields of expertise. The institution was described as *way too small* to manage its responsibilities and an ever-increasing workload. The Acting Director will launch a strategic reflection with managers on how to increase resources in the medium-term. We also need to ensure that we take a very selective approach to new challenges, while continuing to train existing staff to help them expand their expertise. The EDPS might also benefit from bringing in advisory bodies with strategic areas of knowledge.

Data protection is an emerging concern in many different areas, such as consumer protection and competition law, and specialists in these areas are looking to develop a coherent approach to data protection. As pointed out by one stakeholder: *we do not need academic excellence from the EDPS, we need practical, expert advice on our real-world needs*. We must therefore move beyond our traditional legal approach and urgently develop our expertise on new technologies and their impact, as well as on state operations in the areas of law enforcement, the secret service, judicial investigations and business practices.

The EDPS is in a strong position to influence policies on data protection in Europe. However, even our most optimistic predictions could not have anticipated the vast increase in interest in data protection from outside European borders. The General Data Protection Regulation (GDPR), which will be fully applicable from May 2018, is now perceived by many as a global standard. Our responsibility for organising the 2018 International Conference of Data Protection and Privacy Commissioners also reflects the EU's position as an international leader in this area. Taking this into account, it might be appropriate to revisit elements of the Strategy to ensure they better reflect the international environment in which we find ourselves.

During the Management Away Day, the EDPS leadership made it very clear that the institution will continue to be a consistent and influential voice on data protection across the world, as well as in Europe, for the remainder of the current mandate. Our activities over the past few years have created significant expectations that we must fulfil. The EDPS will approach the second part of the mandate with renewed energy, particularly as we look towards the International Conference of Data Protection and Privacy Commissioners, which we will jointly host in October 2018.

Fig. 8. Interview questions for EDPS strategic review

Annex A - Legal framework

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

Since the entry into force of the Lisbon Treaty on 1 December 2009, Article 16 TFEU must be considered as the legal basis for the EDPS. Article 16 underlines the importance of the protection of personal data in a more general way. Both Article 16 TFEU and Article 8 of the EU Charter of Fundamental Rights 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 the Directive on data protection in the police and justice sectors. Directive 95/46/EC will be fully replaced by the General Data Protection Regulation (GDPR) on 25 May 2018, while a new Regulation on privacy and electronic communications (ePrivacy) is currently under negotiation (see section 4.1).

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 4.4.1).

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

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

European Institute for Gender Equality (EIGE)	*Christos GEORGIADIS*
European GNSS Agency (GSA)	*Triinu VOLMER*
European Railway Agency (ERA)	*Zografia PYLORIDOU*
Consumers, Health and Food Executive Agency (CHAFEA)	*Kalliroi GRAMMENOU*
European Centre for Disease Prevention and Control (ECDC)	*Andrea IBER*
European Environment Agency (EEA)	*Eleni BARLA*
European Investment Fund (EIF)	*Paolo SINIBALDI*
European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)	*Nayra PEREZ*
European Securities and Markets Authority (ESMA)	*Sophie VUARLOT-DIGNAC (Acting)*
European Aviation Safety Agency (EASA)	*Francesca PAVESI*
Executive Agency for Small and Medium-sized Enterprises (EASME)	*Elke RIVIERE*
Innovation and Networks Executive Agency (INEA)	*Caroline MAION*
European Banking Authority (EBA)	*Joseph MIFSUD*
European Chemicals Agency (ECHA)	*Bo BALDUYCK*
European Research Council Executive Agency (ERCEA)	*Cristina GANGUZZA*
Research Executive Agency (REA)	*Evangelos TSAVALOPOULOS*
European Systemic Risk Board (ESRB)	*Barbara EGGL*
Fusion for Energy (ITER)	*Angela BARDENHEWER-RATING*
SESAR Joint Undertaking (SESAR)	*Laura GOMEZ GUTIERREZ*
Electronic Components and Systems for European Leadership (ECSEL)	*Anne SALAÜN*
Clean Sky Joint Undertaking (CLEAN SKY JOINT)	*Bruno MASTANTUONO*
Innovative Medicines Initiative Joint Undertaking (IMI JU)	*Desmond BARRY*
Fuel Cells & Hydrogen Joint Undertaking (FCH)	*Georgiana BUZNOSU*
European Insurance and Occupations Pensions Authority (EIOPA)	*Catherine COUCKE*
European Police College (CEPOL)	*Ioanna PLIOTA*
European Institute of Innovation and Technology (EIT)	*Patricia JUANES BURGOS*
European Defence Agency (EDA)	*Clarisse RIBEIRO*
Body of European Regulators for Electronic Communications (BEREC)	*Ena OSTROSKI (Acting)*
European Union Institute for Security Studies (EUISS)	*Nikolaos CHATZIMICHALAKIS*
European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA)	*Fernando POCAS DA SILVA*
Shift2Rail Joint Undertaking (S2R JU)	*Isaac GONZALEZ GARCIA*
Single Resolution Board (SRB)	*Esther BRISBOIS*
Europol (EUROPOL)	*Daniel DREWER*
EFTA Surveillance Authority (ESA)	*Kjersti SNEVE*
Bio-Based Industries Joint Undertaking (BBI JU)	*Marta CAMPOS ITURRALDE*
The European Union's Judicial Cooperation Unit (EUROJUST)	*Diana ALONSO BLAS*

Annex D - List of prior check and non-prior check Opinions

Administration

Anti-fraud, whistleblowing and finance

- Whistleblowing policy (EIB), 29 November 2017 (2016-0381)
- Visitors database (GSA), 14 November 2017 (2016-1055) - Non Prior Check
- Entry of a Data Subject in the Early Detection and Exclusion System (EC), 4 October 2017 (2016-0864)
- Whistleblowing procedures (EIOPA), 7 August 2017 (2017-0466)
- Whistleblowing procedure (EP), 11 July 2017 (2017-0379)
- Initial processing of alerts (ECJ), 7 July 2017 (2017-0304)
- Whistleblowing procedure (EDA), 20 June 2017 (2017-0381)
- Whistleblowing policy (ENISA), 3 April 2017 (2017-0109)
- Whistleblowing procedure (EUIPO), 29 March 2017 (2016-1056)
- Whistleblowing policy (EBA), 7 February 2017 (2016-1173)
- Administrative inquiries (EMCDDA), 30 January 2017 (2016-0989)
- Whistleblowing policy for staff (ESMA), 11 January 2017 (2016-1042)

Administration and Human Resources

- Activity of the Medical Service (EEAS), 14 December 2017 (2016-0780)
- Complimentary sickness insurance for local Agents in EU Delegations (EEAS), 15 November 2017 (2016-0775)
- Reinforced cooperation between the health services of the CoR and of the EESC (CoR and EESC), update, 20 October 2017 (2017-0185)
- Office Indoor Climate Survey (CoR), 28 July 2017 (2017-0676)
- Management of service mobile telephone invoices (EDA), 28 July 2017 (2017-0338)
- Requests under Article 90 and 24 (EEAS), 10 May 2017 (2017-0262)
- Internal mobility (EIF), 3 April 2017 (2015-1102)
- Confluence - Collaborative administrative situation of accredited Parliamentary Assistants (EP), 13 February 2017 (2016-1060)
- Staff development dialogue (ECDC), update, 20 January 2017 (2015-1108)

CCTV

- Notification for prior checking on video surveillance (ECDC), 7 December 2017 (2017-1065) - Non Prior Check
- Automated vehicle license plate recognition system (ECB), 8 August 2017 (2016-0695)
- Video-surveillance system (CoR and EESC), 1 August 2017 (2017-0662)
- CCTV (GSA), 7 June 2017 (2016-1052)

Evaluation (360° and Staff Appraisal)

- Promotions (CEDEFOP), update, 19 October 2017 (2017-0171)
- Development programme: 360° feedback exercise for Management (EASME), 26 July 2017 (2017-0588)
- Procedures related to 360° (multirater) leadership feedback Report (EIB), update, 3 July 2017 (2017-0580)

- Probation periods and e-probation tool for the management of probationary periods (EIF), 27 June 2017 (2015-1107)
- Promotion and reclassification (EMSA), 3 April 2017 (2016-0396)
- 360° feedback exercise managers (OIB), 3 April 2017 (2016-1130)
- 360° feedback exercise manager (F4E), 28 March 2017 (2016-0535)
- Staff appraisals (EUIPO), 22 March 2017 (2017-0114)
- Ex-ante product quality audits for trademarks and designs (EUIPO), 16 February 2017 (2016-0477)
- 360° programme for managers (ECHA), 20 January 2017 (2016-0002)
- 360° feedback process (FRA), 5 January 2017 (2016-1007)

Grants and Public Procurement

- Grants, Awards, & Management (REA), 3 April 2017 (2013-1306)
- Industry portal (F4E), 21 February 2017 (2013-0809) - Non Prior Check

Recruitment

- Selection procedure of temporary agents, contractual agents and national secondees (EIOPA), 14 December 2017 (2013-0541)
- Appointment and engagement of officials, temporary staff, contract staff and trainees (CdT), update, 20 November 2017 (2016-0377)
- Procedures for appointing members of the Management Committee (EIB), 27 October 2017 (2017-0411)
- Renewal procedure of temporary and contract agent's contracts (EUIPO), 6 October 2017 (2017-0256)
- Selection of temporary staff, contract agents and trainees (CEPOL), 21 September 2017 (2017-0187)
- Selection, recruitment and administrative management of contractual agents in EU delegations (EEAS), 12 June 2017 (2016-0770)
- Selection and use of interim workers (BEREC), 9 February 2017 (2015-1088)
- Selection of the Managing Director and Deputy Managing Director (EFSI), 9 February 2017 (2015-0801)

Core Business

- EU High Level Advisers Programme in Moldova (EC and EEAS), 15 December 2017 (2016-0505/ 2017-0712)
- Feedback Event 2017 (EUIPO), 6 December 2017 (2017-0813)
- Participation to the appointment of the top management of EUIPO Agency (EP), 1 December 2017 (2017-0345)
- Clinical Patient Management System (EC), 6 November 2017 (2017-0804)
- Remuneration policies and credits to senior officials (ECB), 5 September 2017 (2017-0358)
- Virtual Operational Coordination Unit (EC) update, 2 August 2017 (2010-0797)
- Fundamental Rights Platform Advisory Panel elections 2017 (FRA), 28 July 2017 (2017-0427)
- Social Biking: A field study on Physical Activity and Social Networks (EC), 8 March 2017 (2017-0080) - Non Prior Check
- Public Hearings (EMA), 17 January 2017 (2016-0953)
- Test run of the Geographic Information System tool (ECDC), 17 January 2017 (2016-0759)

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

Opinions

Please refer to the EDPS website for translations and executive summaries.

In 2017 the EDPS issued Opinions on the following subjects (date of publication in brackets):

- Opinion on ECRIS-TCN (12 December 2017)
- Proposal for a Regulation on integrated farm statistics (20 November 2017)
- Proposal for a Regulation on the eu-LISA (9 October 2017)
- EDPS Recommendations at the current stage of the ePrivacy Regulation legislative process (5 October 2017)
- Commission Proposal for a Regulation of the European Parliament and of the Council on establishing a single digital gateway (1 August 2017)
- Legislative package repealing the current legal basis of Schengen Information System (SIS) (3 March 2017)
- Proposed ePrivacy Regulation (24 April 2017)
- Regulation 45/2001 (15 March 2017)
- Digital Content (15 March 2017)
- ETIAS (6 March 2017)
- Proposal for a common framework for European statistics relating to persons and households (1 March 2017)
- Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications (anti-money laundering) (2 February 2017)

Formal comments

Please refer to the EDPS website for French and German translations.

In 2017 the EDPS issued formal comments on the following subjects (date of publication in brackets):

- Proposal for a Regulation on the European citizens' initiative (19 December 2017)
- Cybersecurity package (IT Policy unit and Policy & Consultation) (15 December 2017)
- Public consultation on lowering fingerprinting age for the VIS (19 November 2017)
- Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and the Council with regard to "the provision of EU-wide multimodal travel information services" (22 August 2017)
- Proposal under consideration to amend Regulations (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems ("the basic Regulation") and its implementing Regulation, Regulation (EC) No 987/2009 ("the implementing Regulation") (8 May 2017)
- (Letter) Proposed Regulation of the European Parliament and of the Council on controls on cash entering or leaving the union and repealing Regulation (EC) no 1889/2005 (21 February 2017)

Other documents

Please refer to the EDPS website for French and German translations.

In 2017, the EDPS issued papers on the following subjects (date of publication in brackets):

- Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice (17 November 2017)
- Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (11 April 2017)

Annex F - Speeches by the Supervisor and Assistant Supervisor in 2017

European Parliament

Assistant Supervisor, *LIBE Progress towards the interoperability of EU information systems*, speech by Wojciech R. Wiewiórowski, Brussels (21 November 2017)

Supervisor, Joint Parliamentary Scrutiny Group of Europol, address by Giovanni Buttarelli to the constituent meeting of the Joint Parliamentary Scrutiny Group of Europol, European Parliament, Brussels (9 October 2017)

Supervisor, *The state of privacy 2017: mid-mandate report*, speech by Giovanni Buttarelli for the presentation of the 2016 EDPS Annual Report to the LIBE Committee, European Parliament, Brussels, (4 May 2017)

Supervisor, Meeting with EP rapporteur and shadow rapporteurs on new EUI Regulation - presentation of EDPS Opinion 5/2017, European Parliament, Brussels (3 May 2017)

Supervisor, Hearing on ePrivacy, LIBE Committee, European Parliament, Brussels (11 April 2017)

Supervisor, Proposed Digital Content Directive, speech by Giovanni Buttarelli addressed to Socialists & Democrats Group workshop, European Parliament, Brussels (12 January 2017)

Council

Supervisor, New EUI Regulation - presentation of EDPS Opinion to DAPIX, Brussels (23 March 2017)

Assistant Supervisor, Council Working Party on Financial Services (AMLD), *Access to beneficial ownership information and data protection implications,* speech by Wojciech R. Wiewiórowski, Brussels (13 March 2017)

Supervisor, Directive on digital content - invitation to present at the Council WP, Brussels (22 February 2017)

European Commission

Supervisor, Mentor Group Brussels Forum for EU-US Legal-Economic Affairs, Brussels (3-5 April 2017)

Other EU institutions and bodies

Assistant Supervisor, *Financial Markets and Data Protection*, at the seminar *Data Protection*, European Central Bank, Frankfurt, Germany (25-26 October 2017)

Assistant Supervisor, *The False Dichotomy of Security v. Privacy*, at ENISA Annual Privacy Forum 2017, Vienna, Austria (7-8 June 2017)

International conferences

Assistant Supervisor, *Surveillance for Public Security Purposes. Four pillars of acceptable interference in fundamental right to privacy*, at the conference *Privacy challenges related to EU-level security, control and surveillance mechanisms*, Gent, Belgium (12 December 2017)

Supervisor, 8th Annual Data Protection and Privacy Conference, speech by Giovanni Buttarelli, Brussels (30 November 2017)

Supervisor, European Business Summit "Think Digital", keynote speech by Giovanni Buttarelli, Brussels (28 November 2017)

Assistant Supervisor, *No Silver Bullet: Accidental and Essential Problems of Privacy Engineering*, at the conference *Privacy Engineering Research and the GDPR: A Trans-Atlantic Initiative*, Leuven, Belgium (10 November 2017)

Assistant Supervisor, *Efficiency of the Data Protection Regulations in the Light of Experiences* (Skuteczność regulacji ochrony danych osobowych w świetle dotychczasowych doświadczeń), at the International Conference on the occasion of the 20th anniversary of the personal data protection law in Poland: *Unchanging Values and their Effective Protection in the Era of*

Changes (Niezmienne wartości i ich skuteczna ochrona w dobie przemian), Warsaw, Poland (17 October 2017) (recording: begins at 1:12:30)

Supervisor, speech by Giovanni Buttarelli to AIPPI (International Association for Protection of Intellectual Property) via video message, Sydney, Australia (15 October 2017)

Supervisor, 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC), presentation by Giovanni Buttarelli, Hong Kong (29 September 2017)

Assistant Supervisor, *Ethics by Design in Artificial Intelligence?* at the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC), Hong Kong (25-29 September 2017)

Assistant Supervisor, *Operationalise Accountability and Privacy by Design: What to Automate in Your Privacy Programme*, at the 39th International Conference of Data Protection and Privacy Commissioners, Hong Kong (25-29 September 2017)

Assistant Supervisor, *EU Policy Framework on Cybersecurity and Data Protection*, at the 1st Annual CSCG/ENISA Workshop, Brussels (19 September 2017)

Assistant Supervisor, *Artificial intelligence in legal profession*, at the conference *Looking to the European Union of the future; renovation and/or innovation*, Cambridge, United Kingdom (8 September 2017)

Assistant Supervisor, *Policy for data in the EU - bottleneck and expectations*, at the conference *Digital Single Market Conference on the Free Movement of Data*, Tallinn, Estonia (17 July 2017)

Supervisor, Privacy Laws & Business 30th Anniversary Conference, Cambridge, United Kingdom (5 July 2017)

Assistant Supervisor, *Fair and lawful processing: Understanding the logic behind Artificial Intelligence algorithms*, at the conference *Privacy Laws & Business: Promoting Privacy with Innovations*, Cambridge, United Kingdom (3-5 July 2017)

Supervisor, speech to the Italian Senate, Senato della Repubblica, 8ª Commissione Lavori pubblici, comunicazioni, Rome, Italy (14 June 2017)

Assistant Supervisor, *Sensitive Processing of Non-Sensitive Data, Business analytics tools in financial sector*, at a seminar on *The Innovative use of data in retail financial services*, Brussels (6 June 2017)

Assistant Supervisor, *Data privacy - challenges in internal cross border investigations and criminal defence work*, lecture at the 20th IBA Annual Transnational Crime Conference, Lisbon, Portugal (17-19 May 2017)

Supervisor, *19th Meeting of the Central and Eastern European DPAs*, speech by Giovanni Buttarelli at the 19th Meeting of the Central and Eastern European Data Protection Authorities (CEEDPA) in Tbilisi, Georgia (17 May 2017) (recorded)

Supervisor, *Hitting the ground running: How regulators and businesses can really put data protection accountability into practice*, keynote speech by Giovanni Buttarelli at European Data Protection Days (EDPD) Conference, Berlin, Germany (15 May 2017)

Assistant Supervisor, *The GDPR & Convention 108's new guidelines: meeting the challenges of Big Data*, at the ERA Annual Conference On European Data Protection Law 2017: *Focus on the General Data Protection Regulation*, Brussels (11-12 May 2017)

Assistant Supervisor, *Ensuring safe and efficient international data transfers in a globalised world: current issues and how to make it work*, at the ERA Annual Conference On European Data Protection Law 2017: *Focus on the General Data Protection Regulation*, Brussels (11-12 May 2017)

Supervisor, *Workshop: Data Protection within International Organizations*, opening speech, organised by the International Organization for Migration and the European Data Protection Supervisor, Geneva, Switzerland (11 May 2017)

Supervisor, Spring Conference of Data Protection Authorities, Limassol, Cyprus (26 April 2017)

Supervisor, *The Future of European Privacy, Security, and Surveillance Policies*, Council on Foreign Relations, Washington D.C., United States (17 April 2017)

Assistant Supervisor, *Building a Data Economy. Data Protection Issues*, at the conference *Emerging Legal Issues in an Increasingly Digital Society*, Hull, United Kingdom (30-31 March 2017)

Supervisor, *10th Computers, Privacy and Data Protection Conference (CPDP)*, concluding remarks, Brussels (27 January 2017)

Supervisor, ch@rterclick! project the EU charter in the everyday activity of the national data protection authorities: experiences, problems, perspectives, video message as part of the *Interactive Key-Note Panel: Plurality of legal instruments governing data protection – objectives, interactions, added value*, Florence, Italy (20 January 2017)

Other events

Supervisor, *Think Digital Summit*, Brussels (28 November 2017)

Supervisor, Expert Workshop EUI, Florence, Italy (24 November 2017)

Supervisor, *Trattamento dei dati personali e Privacy Officer*, Bologna, Italy (21 November 2017)

Supervisor, *Administrative transparency and Access to Information 2017*, videoconference, Milan, Italy (13 November 2017)

Supervisor, *Privacy Engineering Research and the GDPR: A Trans-Atlantic Initiative*, opening speech at the workshop *Privacy Engineering Research and the GDPR: A Trans-Atlantic Initiative*, Leuven, Belgium (10 November 2017)

Supervisor, *Data Protection e Reg. UE 2016/679: la privacy nell'Europa 4.0*, Turin, Italy (6 November 2017)

Supervisor, *Vittorio Frosini: una coscienza giuridica aperta al futuro*, Rome, Italy (27 October 2017)

Supervisor, *Il regolamento generale sulla protezione dei dati (Reg. UE n. 2016/679)*, Rome, Italy (26 October 2017)

Assistant Supervisor, *Borderline between public and private sector needs and privacy protection* (Granica między potrzebami sektora publicznego i prywatnego, a koniecznością zapewnienia ochrony prywatności osób), at the conference *Data Protection System Reform - GDPR generated challenges for Poland* (Reforma systemu ochrony danych osobowych – wyzwania dla Polski w związku z RODO), Warsaw, Poland (22 September 2017) (video)

Assistant Supervisor, *The new Data Protection* Regulation, at the European Regulatory Workshop Programme of Eurofinas – the European Federation of Finance House Associations and Leaseurope - the European Federation of Leasing Company Associations, Brussels (29 June 2017)

Assistant Supervisor, *The Ocean That Connects Us, Trans-Atlantic Perspectives on Privacy*, at the conference *Trans-Atlantic Data Privacy Relations As A Challenge For Democracy*, Brussels (28 June 2017)

Assistant Supervisor, *Compliant or/and Accountable in Privacy by Design Environment*, at the seminar *European Parliament Data Protection Day, Managing accountability and compliance in the Reform Era*, Brussels (28 June 2017)

Assistant Supervisor, *Non Autonomous Data. Who Controls Smart Car in the Smart City?* at the seminar *Autonomous Driving and Data: Access, Ownership, Security*, Brussels (27 June 2017)

Assistant Supervisor, *Regulators' View. The Accountability principle: What strengthening corporate responsibility entails*, at the conference *DPOs 3rd International Roundtable: From privacy by design to data breach notification: Your top priorities to be GDPR-compliant by May 2018*, Paris, France (23 June 2017)

Assistant Supervisor, *Privacy by Design in Theory and in Real World*, at the 5th Workshop of the Internet Privacy Engineering Network (IPEN), Vienna, Austria (9 June 2017) (video)

Supervisor, FutureTech Congress in Warsaw, speech on the panel *The impact of the GDPR on solutions based on Big Data processing*, Warsaw, Poland (25 May 2017)

Assistant Supervisor*, Implementation of the GDPR in Telecom Sector*, at the ETNO – the European Association of Telecom Network Operators - DPOs Summit, Brussels (24 May 2017)

Assistant Supervisor, *Impact of the GDPR for vehicle and driver licence registration authorities. Will guidelines and codes of conduct help in practical implementation?* at the EReg Academy on Data Protection, Brussels (15 May 2017)

Supervisor, Invitation as Guest Speaker - INSEAD Alumni Association, Rome, Italy (9 May 2017)

Supervisor, Congresso ASSO DPO 2017, speech, Milan, Italy (8 May 2017)

Supervisor, CONVEGNO-TAVOLA ROTONDA PRIVACY - UNIMIB, Milan, Italy (8 May 2017)

Assistant Supervisor, *Data Protection and International Exchange of Information on Criminal Proceedings*

(Ochrona danych osobowych przy międzynarodowej wymianie informacji dotyczących postępowań karnych) at the Scientific Conference Legal Innovation, Wroclaw, Poland (21-22 April 2017)

Assistant Supervisor, *Re-use of maritime passengers' PNR data for public security purposes* (Wtórne przetwarzanie na potrzeby bezpieczeństwa publicznego danych PNR, dotyczących osób odbywających podróż morską), at the VI Polish Conference of Maritime Law: Maritime Safety, Gdansk, Poland (20 April 2017)

Assistant Supervisor, *Data Protection Authority 2.0. New place, mission, competences and tools* (Organ ochrony danych osobowych 2.0. Nowe miejsce, misja, zadania i narzędzia działania), at the conference *GDPR, Innovation, Security and Audit: Challenges of data protection in times of new regulations* (RODO, Innowacje, Bezpieczeństwo, Audyt - RIBA'2017. Wyzwania ochrony danych w czasach nowych regulacji), Warsaw, Poland (6-7 April 2017) (video)

Assistant Supervisor, *General Data Protection Regulation - personal data protection in the era of digital society* (Ogólne Rozporządzenie o Ochronie Danych – ochrona danych osobowych w erze społeczeństwa cyfrowego), at the 2nd Polish Cyber Security Forum – CYBERSEC PL, Warsaw, Poland (6 April 2017) (video)

Assistant Supervisor, *Impact of the Supervisor's decisions strengthening the Digital Single Market*, at the Forum for EU-US Legal-Economic Affairs, Brussels (4-6 April 2017)

Supervisor, *All we need is L….Privacy by design and by default*, opening speech at RightsCon 2017, Brussels (29 March 2017)

Assistant Supervisor, *Towards a new digital ethics – data, dignity and technology: How to ensure accountability in personal data management?* at the conference *The regulation of privacy through ethical standards and accountability in the era of Big Data*, Brussels (13-14 March 2017)

Supervisor, Privacy Day at ICANN58, Copenhagen, Denmark (13 March 2017)

Supervisor, opening statement for panel on Digital Rights and Enforcement, 10th Computers, Privacy and Data Protection Conference, Brussels (26 January 2017)

Supervisor, Ethics, research and the data-driven society, speech at the ESOMAR European Insights Summit, Brussels (24 January 2017)

Annex G - Composition of EDPS Secretariat

Director and Private Office

Christopher DOCKSEY*
Director

Leonardo CERVERA NAVAS
Acting Director

Christian D'CUNHA
Policy Assistant to the EDPS

Ernani CERASARO
Policy Administrative Assistant

Anna COLAPS
Policy Assistant

Sylvie PICARD
Internal Control Coordinator

Maria José SALAS MORENO
Administrative Assistant

Martine VERMAUT
Administrative Assistant

Supervision and Enforcement

Maria Veronica PEREZ ASINARI
Head of Unit

Isabelle CHATELIER*
Head of Complaints and Litigation

Petra CANDELIER
Head of Complaints and Litigation

Bénédicte RAEVENS
Head of EUROPOL Supervision

Ute KALLENBERGER
Head of Inspections

Owe LANGFELDT
Acting Head of Prior checks and Consultations

Stephen ANDREWS
Supervision and Enforcement Assistant

Guillaume BYK
Legal Officer

Fanny COUDERT
Legal Officer

Elena FIERRO
Legal Officer

Mario GUGLIELMETTI
Legal Officer

Delphine HAROU
Legal Officer

Dirk HOMANN
Legal Officer

Xanthi KAPSOSIDERI
Legal Officer

Francoise MAYEUR
Supervision and Enforcement Assistant

Anna LARSSON STATTIN
Legal Officer/Seconded National Expert

Snezana SRDIC
Legal Officer

Tereza STRUNCOVA
Legal Officer

Zsofia SZILVASSY
Legal Officer

Policy and Consultation

Sophie LOUVEAUX
Head of Unit

Anna BUCHTA
Deputy Head of Unit

Anne-Christine LACOSTE
Head of International Cooperation

Olivier MATTER
Team Leader for International Cooperation

Amanda JOYCE
Policy and Consultation Assistant

Zsuzsanna BELENYESSY
Legal Officer

Priscilla DE LOCHT
Legal Officer

Alba BOSCH MOLINE *
Legal Officer

Claire GAYREL
Legal Officer

Jacob KORNBECK*
Legal Officer

Laurent LIM
Legal Officer

Fabio POLVERINO*
Legal Officer

Lara SMIT
Legal Officer

IT Policy

Achim KLABUNDE
Head of Sector

Fredrik LINDHOLM
Administrative Assistant

Massimo ATTORESI
Technology and Security Officer
Data Protection Officer

Andy GOLDSTEIN
Technology and Security Officer
LISO

Dina KAMPOURAKI
Technology and Security Officer

Malgorzata LAKSANDER
Technology and Security Officer

Fidel SANTIAGO*
Technology and Security Officer

Xabier LAREO
Technology and Security Officer/Seconded National Expert

EDPB Matters

Isabelle VEREECKEN
Acting Head of Sector

Katinka BOJNAR
Legal Officer/Seconded National Expert

Zoi KARDASIADOU
Legal Officer/Seconded National Expert

Peter KRAUS
Technology and Security Officer

Fabienne MOLLET
Administrative Assistant

Romain ROBERT
Legal Officer

Andrei PETROVICI
Technology and Security Assistant

Anna ZAWILA- NIEDZWIECKA
Legal Officer/Seconded National Expert

Records Management

Luisa PALLA
Head of Sector

Marta CÓRDOBA HERNÁNDEZ
Administrative Assistant

Denisa IONICA*
Administrative Assistant

Kim Thien LÊ
Administrative Assistant

Anne NOEL
Administrative Assistant

Séverine NUYTEN
Administrative Assistant

Sonya SOMRANI PEREZ*
Administrative Assistant

Maria TIGANITAKI
Administrative Assistant

Information and Communication

Olivier ROSSIGNOL
Head of Sector

Francesco ALBINATI
Information and Communication Officer

Thomas HUBERT
Graphic Designer

Courtenay MITCHELL
Information and Communication Officer

Parminder MUDHAR
Information and Communication Officer

Agnieszka NYKA
Information and Communication Officer

Benoit PIRONET
Web Developer

Human Resources, Budget and Administration

Marian SANCHEZ LOPEZ
Acting Head of Unit

Cláudia BEATO
HR Assistant

Pascale BEECKMANS
HR Assistant
GEMI

Laetitia BOUAZZA-ALVAREZ
HR Assistant
GECO
LSO
Traineeship Coordinator

Julia MOLERO MALDONADO
Finance Assistant

Marco MORESCHINI
HR Officer/Seconded National Expert
LSO

Carolina POZO LOPEZ
Finance Assistant

Karina REMPESZ
HR Officer
L&D Coordinator

Anne-Françoise REYNDERS
HR Officer

Caroline WOUSSEN-DUBUISSEZ
Finance Assistant

*staff members who left the EDPS in the course of 2017

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: https://europa.eu/european-union/contact_en

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

www.edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

EDPS

European Data Protection Supervisor

Publications Office