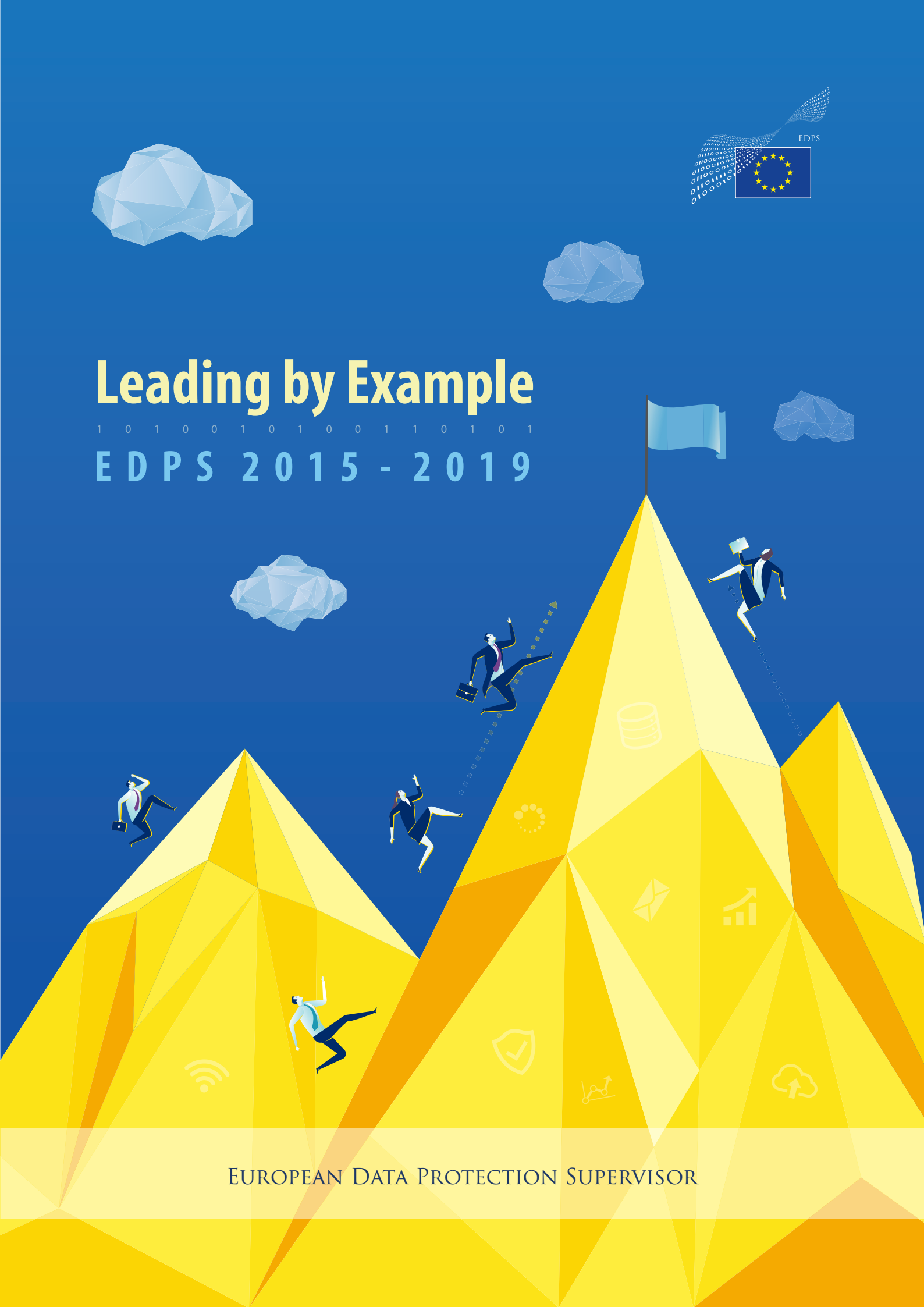


Leading by Example

1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1

EDPS 2015 - 2019

European Data Protection Supervisor

An Executive Summary of this report, which gives an overview of key developments in EDPS activities during the 2015-2019 mandate, is also available.

Further details about the EDPS can be found on our website at www.edps.europa.eu

Details on how to subscribe to the EDPS Newsletter can also be found on the website.

Luxembourg: Publications Office of the European Union, 2019

Print: ISBN 978-92-9242-445-9 doi:10.2804/956616 QT-04-19-470-EN-C
PDF: ISBN 978-92-9242-450-3 doi:10.2804/386075 QT-04-19-470-EN-N
HTML: ISBN 978-92-9242-449-7 doi:10.2804/268776 QT-04-19-470-EN-Q

Leading by Example

1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1

EDPS 2015 - 2019

CONTENTS

FIGURES

FOREWORD

Giovanni Buttarelli and I issued a Strategy for our mandate within 100 days of taking up our posts.

The content of this short document reflected our vision for privacy in the digital age. It was a vision of an EU with world-class data protection standards, leading by example. It saw the EDPS, in our role as a supervisory authority and policy advisor, as a centre of excellence for data protection.

Over the past five years, people and policymakers have become increasingly aware of the reality and potential of digital technology.

Edward Snowden's revelations in 2013 exposed the depth and breadth of state intrusion into our private lives. The Facebook/Cambridge Analytica scandal in 2018 revealed the fragility of our democracy, where the public sphere has shifted onto a complex, unaccountable matrix of tracking, profiling and targeting. The most highly valued companies in the world are now those who have been most successful in collecting and monetising personal information, while acquiring thousands of start-ups that might have posed competition and diversified the business models available.

We now know that the hidden price of the much-vaunted convenience of digitisation is unsustainable and often unscrupulous data practices and a growing divide between winners and losers. The side effect of connecting the world has been opaque revenue-maximising algorithms, which serve as agents of social division and tools of oppression.

Many regions of the world, not only the EU, are now examining how they can give people more control over their data and digital lives, and introduce discipline into markets which, for almost 20 years, had been allowed to develop and disrupt with minimal oversight. At the beginning of our mandate, South Africa had just become the 101st country to adopt a comprehensive data privacy law. This year Nigeria became the 134th.

Our watchword over the past five years has been accountability. Accountability of controllers for what they do with the personal data of others, and accountability of supervisory authorities in exercising, with integrity and consistency, the enhanced powers entrusted to us by the General Data Protection Regulation (GDPR).

Our Strategy was also an exercise in accountability for the objectives we said we would pursue and the priority actions we said we would carry out – focusing on digitisation, global partnerships and modernising data protection. On many levels, I believe that we delivered.

We have investigated EU bodies' contractual relationships with service providers, established a forum for agencies to exchange views on the regulation of digital markets and ensured that the new European Data Protection Board (EDPB) had the necessary resources to carry out its work. Above all, we have propelled the question of ethics and new technologies, particularly Artificial Intelligence, to the centre of public policy debate.

I would like to pay tribute to our excellent and dedicated staff who were instrumental in our efforts to turn our vision into a reality on the ground.

However, we must remember that this is only the start of what will be a very long process. Over the coming years, we face the challenge of ensuring that individuals are able to exercise more control over their digital lives and of making personal data work for society in general, not just for a handful of powerful private interests.

Wojciech Wiewiórowski
Assistant European Data Protection Supervisor

1. ABOUT THE EDPS

The European Data Protection Supervisor (EDPS) ensures that the European Union's institutions, offices, bodies and agencies respect the fundamental rights to privacy and data protection, whether they process personal data or are involved in developing new policies that may involve the processing of personal data. The EDPS has four main fields of work:

- **Supervision:** We monitor the processing of personal data by the EU administration and ensure that they comply with data protection rules. Our tasks range from conducting investigations to handling complaints and prior consultations on processing operations.
- **Consultation:** We advise the European Commission, the European Parliament and the Council on proposals for new legislation and other initiatives related to data protection.
- **Technology monitoring**: We monitor and assess technological developments, where they have an impact on the protection of personal data, from an early stage, with a particular focus on the development of information and communication technologies.
- **Cooperation:** Among other partners, we work with national data protection authorities (DPAs) to promote consistent data protection across the EU. Our main platform for cooperation with DPAs is the European Data Protection Board (EDPB), for which we also provide the secretariat.

Up until 11 December 2018, the EU institutions had to comply with the data protection rules set out in Regulation 45/2001. On 11 December 2018, Regulation 45/2001 was replaced by Regulation (EU) 2018/1725. It is the job of the EDPS to enforce these rules.

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

For Member State law-enforcement bodies, the applicable law is Directive 2016/680, on data protection in the police and criminal justice sectors. Article 3 and Chapter IX of Regulation 2018/1725 apply to the processing of operational personal data by EU bodies, offices and agencies involved in police and judicial cooperation, and these provisions are closely modelled on the rules set out in Directive 2016/680.

In addition to this, separate rules exist concerning the processing of personal data for operational activities carried out by the EU's law enforcement agency, Europol. These activities include the fight against serious crime and terrorism affecting more than one Member State. The relevant legislation in this case is Regulation 2016/794, which also provides for EDPS supervision of these data processing activities. As for the other EU institutions and bodies, the EDPS is also responsible for supervising the processing of personal data relating to Europol's administrative activities, including personal data relating to Europol staff, under Regulation 2018/1725. A similar, specific, data protection regime is in place for the European Public Prosecutor's Office and Eurojust.

2. EDPS STRATEGY 2015-2019

The EDPS Strategy 2015-2019 defined our priorities for the mandate and provided a framework through which to promote a new culture of data protection in the EU institutions and bodies. It summarised:

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

In order to achieve our vision of an EU that leads by example in the global dialogue on data protection and privacy in the digital age, we set out three strategic objectives and ten action points:

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

(1) developing an ethical dimension to data protection;
(2) speaking with a single EU voice in the international arena;
(3) mainstreaming data protection into international policies.

3 Opening a new chapter for EU data protection

(1) adopting and implementing up-to-date data protection rules;
(2) increasing the accountability of EU bodies collecting, using and storing personal information;
(3) facilitating responsible and informed policymaking;
(4) 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

3. 2015-2019 ACHIEVING OUR VISION

Data protection affects almost every EU policy area. It also plays a key role in legitimising and increasing trust in EU policies. Europe is the world's leading proponent for the protection of fundamental rights and human dignity. It is therefore vital that the EU plays a leading role in shaping a global standard for privacy and data protection, centred on these values.

Giovanni Buttarelli was appointed European Data Protection Supervisor by joint decision of the European Parliament and the Council on 4 December 2014. Assistant Supervisor Wojciech Wiewiórowski was appointed on the same date. Set to serve for a five-year term, they faced the challenging task of facilitating the EU's transition to a new era in data protection practice.

With this in mind, their first action as EDPS and Assistant Supervisor was to develop a strategy for the five-year mandate (see chapter 2). On 2 March 2015, we published the EDPS Strategy 2015-2019, presenting it at an event attended by EU Commissioners and other influential stakeholders. The hard work of putting the Strategy into practice then began.

3.1 Seeing in a new era for EU data protection policy

At the beginning of the mandate, talks on a new framework for EU data protection had stalled. One of our first priorities was therefore to assist the European Commission, the Parliament and the Council in resolving their differences and coming to an agreement (see section 6.1).

Acting in our role as an advisor to the EU legislator, we not only published article-by-article recommendations on the proposed texts for the General Data Protection Regulation (GDPR), we also provided these recommendations in the form of a mobile app. Used by negotiators as a reference guide, the app also helped in promoting greater legislative transparency.

Agreement on the text of the GDPR and the Directive for data protection in the police and justice sectors came in December 2015 and the final texts were published in May 2016. Preparations therefore began in 2016 to ensure that the EU would be ready to implement the new rules when they became fully applicable in May 2018. This involved both drafting guidance on the new rules and setting up the new European Data Protection Board (EDPB), for which the EDPS would provide the secretariat.

Working in close cooperation with our colleagues in the Article 29 Working Party (WP29), we were able to ensure that the EDPB was up and running in time for the GDPR's launch day on 25 May 2018 (see section 6.1.3). In addition to taking on several new tasks aimed at ensuring the consistent application of the GDPR across the EU, the EDPB replaced the WP29 as the main forum for cooperation between the EU's national data protection authorities (DPAs) and the EDPS.

The GDPR applies to organisations and businesses operating within the EU Member States. It does not, however, apply to the EU institutions themselves, who are subject to a different set of rules. In 2017, with preparations for the GDPR well underway, we stepped up our efforts to support the EU legislator in revising the rules applicable to the EU institutions, in order to bring them in line with the GDPR.

However, the legislators were not able to agree on what would become Regulation 2018/1725 until May 2018. The new rules for the EU institutions did not, therefore, come into force until 11 December 2018, just over six months after the GDPR became fully applicable (see section 6.1.4).

The GDPR, the Directive for data protection in the police and criminal justice sectors and Regulation 2018/1725 follow the same principles. The EDPS, as the data protection supervisor for the EU institutions, was therefore able to make an educated guess at what the revised rules for the EU institutions would entail and to start preparing the EU institutions for their new responsibilities at an early stage.

Preparations included providing training sessions, visits and guidance on the new rules. Our main focus was on the principle of accountability, which involved ensuring that the EU institutions not only complied with the new rules, but that they could also demonstrate this compliance (see section 6.2). We wanted to ensure that the EU institutions were ready to lead by example in applying data protection rules, setting the standard for others in the EU to follow.

Efforts to reach an agreement on a Regulation for electronic privacy (ePrivacy), were less successful, however. Though the EDPS went to great lengths to encourage the co-legislators to move forward with this file, coming to a final agreement on the text before the European Parliament elections in May 2019 ultimately proved impossible.

One area that Regulation 2018/1725 does not cover is the processing of operational personal data at the EU's law enforcement body, Europol. Under the Europol Regulation, the EDPS took on responsibility for this task on 1 May 2017. Over the past two-and-a-half years, the EDPS has built up a constructive relationship with Europol, helping them to fulfil their statutory tasks, without compromising the fundamental rights to data protection and privacy (see section 6.4.3).

3.2 An international approach to data protection

In the digital world, however, legislation alone is no longer sufficient. Traditional frameworks used to ensure respect for fundamental rights may not be robust enough to withstand the challenges posed by the digital revolution. In the EDPS Strategy, we therefore committed to launching a global debate on how we can ensure the protection of fundamental rights and values in the digital age, through developing an ethical dimension to data protection.

To address this, we launched the EDPS Ethics Initiative (see section 5.1). In an Opinion published on 11 September 2015, we called for the development of a new digital ethics, putting human dignity at the heart of personal, data-driven technological development. The Opinion also announced our intention to set up an Ethics Advisory Group (EAG), a group of experts from different backgrounds tasked with exploring the relationships between human rights, technology and markets, and identifying threats to the rights to data protection and privacy in the digital era.

The EAG was formed in early 2016, and in early 2018 they published their final report, reflecting on the issues at stake. We followed this up with a public consultation on digital ethics, designed to open up the debate to all sections of society, across the world.

As co-hosts of the 2018 International Conference of Data Protection and Privacy Commissioners, we decided to dedicate the public session of the conference to the topic of Digital Ethics. Our aim was to build on the work produced through the Ethics Initiative to instigate a global debate on the challenges of the digital age.

To capitalise on the success of the conference, in 2019 we launched a podcast. Each #DebatingEthics Conversation explored a specific area of concern identified at the conference and led to the publication of a second Opinion on Digital Ethics in late 2019. With the topic now firmly established on the international data protection agenda, we look forward to further developments in this area in the near future.

However, it is not only in the area of digital ethics that our efforts to engage with international partners have intensified. Better relationships with the European Commission, the European Parliament and the Council mean that we are now consulted much more frequently on proposed EU policy, including international policies, and that we do not hesitate to make our voice heard in cases where we have valid concerns that are not being taken into account.

A guide to current EU data protection rules

EU data protection law is set out in a number of EU Regulations and Directives. Though the rules for private and public organisations operating in the Member States are similar to those governing data protection in the EU institutions, they are not the same. Here we list the rules currently in place in the EU and to which types of organisations they apply.

The General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679: Applicable to the majority of public and all private organisations operating in the EU's Member States. These rules are enforced by the relevant Member State's independent national data protection authority (DPA).

Regulation (EU) 2018/1725: Applicable to all EU institutions, bodies, offices and agencies. These rules are enforced by the European Data Protection Supervisor (EDPS).

Directive (EU) 2016/680 on data protection in the areas of police and criminal justice: Applicable to law enforcement activities carried out by the competent bodies in the EU Member States. Enforced by the relevant Member State's independent national DPA.

Article 3 and Chapter IX of Regulation (EU) 2018/1725: Applicable to the processing of personal data for law enforcement purposes by an EU institution, body, office or agency. These rules are enforced by the EDPS.

Regulation (EU) 2016/794 on Europol: Sets out the rules for the processing of operational personal data at the EU's law enforcement agency, Europol. These rules are enforced by the EDPS.

Regulation (EU) 2017/1939 on EPPO: Sets out the rules for the processing of operational personal data at the European Public Prosecutor's Office. These rules will be enforced by the EDPS.

Regulation (EU) 2018/1727 on Eurojust: Sets out some specific rules that Eurojust will apply in certain specific cases, from 12 December 2019. In all other cases, Chapter IX of Regulation (EU) 2018/1725 will apply to its operational activities. These rules will be enforced by the EDPS.

Directive 2002/58/EC on data protection and privacy in electronic communications (ePrivacy): Sets out the rules for data protection and privacy in the electronic communications sector. Certain rules, such as those on the processing of traffic and location data, apply only to telecom operators and internet service providers. Other rules, such as confidentiality, online tracking and spam, are applicable to all public and private organisations operating in the Member States. Article (5(3)) applies directly to EU institutions.

With the EDPB now in place, the EU is also better able to coordinate its efforts and synchronise its messages on data protection, giving us a stronger voice on the international stage.

3.3 A collaborative response to the digital challenge

Our technological capabilities are developing at an increasingly rapid pace. The progress made in the five years since the start of the EDPS mandate is astounding in itself. Yet, while new technologies have profoundly changed the way we live, determining how best to regulate the development of these technologies is not an easy task.

Through the Internet Privacy Engineering Network (IPEN), which brings together experts from a range of different areas, the EDPS has endeavoured to promote technologies that enhance privacy and data protection. By facilitating the implementation of the principles of data protection by design and by default, obligatory under the GDPR, the data protection Directive for the police and justice sectors and Regulation 2018/1725, the Network aims to ensure that data protection is built in to the design and development of all new technologies (see section 4.1.1).

The EDPS also aims to develop and share technological expertise in the area of data protection, whether through Opinions, Comments, briefing papers or our TechDispatch Newsletter (see section 4.1.2).

The Digital Clearinghouse is another of our collaborative initiatives. Set up by the EDPS in 2016, and officially launched the year after, the Clearinghouse meets twice a year and acts as a forum for cooperation between competition, consumer and data protection authorities. Through working together, it is hoped that regulators in these fields will be better able to address the challenges posed by the digital economy and coherently enforce EU rules relating to fundamental rights in the digital world (see section 4.2.1).

Leading by example, however, starts with the EU institutions. As their supervisory authority, it is up to us to ensure that they set the standard for others to follow, by helping them to increase the accountability and transparency of their work. Through providing training and guidance and working in close cooperation with the data protection officers (DPOs) of the EU institutions, we aim to provide them with the tools to do this. We also monitor the activities of EU institutions and bodies closely and in 2019, we launched two high-profile investigations. These were aimed at ensuring that the EU institutions uphold the highest levels of data protection compliance, thus ensuring the highest levels of protection for all individuals living in the EU (see section 4.3.1).

Through our work with the EU institutions, we hope not only to improve the data protection practices of the EU institutions, but to contribute to efforts to improve data protection across the EU and globally, by increasing awareness of data protection principles, as well as possible issues and concerns.

3.4 Delivering the strategy

Careful resource management and effective communication were integral to achieving the objectives set out in the EDPS Strategy. In this way, we were able to ensure that we had adequate resources to carry out the work involved and that our messages reached the intended audiences.

At the very beginning of the mandate, we engaged in a re-branding project (see section 7.1.1). We wanted to develop a new visual identity for the institution that would reflect our status as a leading global voice on data protection and privacy. The first stage of the project was completed in 2015, with the development of a new logo. We launched a new website, incorporating a new, user-friendly layout, in March 2017, and followed this with a new approach to our Newsletter in June 2017. New initiatives such as a blog and the EDPS app also contributed to providing greater transparency about the work of the EDPS and EU policy in general.

In order to take on new responsibilities and perform them to a high standard, the EDPS needed to hire more data protection experts

(see section 7.2.1). Through the organisation of two competitions for data protection experts through the European Personnel Selection Office (EPSO), we were able to ensure that we had a list of competent data protection experts to draw from to fill any vacancies. This was particularly helpful in setting up the EDPB Secretariat. In addition, we have invested time and effort in developing the skills and knowledge of our existing staff members to ensure that we are able to lead the way in data protection accountability.

As an EU institution itself, the EDPS is also bound by the new data protection rules for the EU institutions. Our credibility and authority as the EU data protection authority depends on us implementing these rules to the highest of standards. Institution-wide collaboration was therefore required in order to ensure we were prepared to lead the way in accountable data protection compliance.

3.5 Key performance indicators

After the adoption of our Strategy 2015-2019 in March 2015, we re-evaluated our existing key performance indicators (KPIs) and established a new set of KPIs, reflecting our new strategic objectives and priorities. They were designed to help us to monitor and adjust, where needed, the impact of our work and the efficiency of our use of resources.

Throughout the mandate, we reported on our KPIs on a yearly basis, in our Annual Report. Some KPIs were adapted to reflect changes or relevant developments affecting the performance of some activities.

The KPIs referring to the first strategic objective (*Data protection goes digital*) focused on initiatives promoting technologies to enhance

Objective 1 - *Data protection goes digital*

Number of initiatives promoting technologies to enhance privacy and data protection organised or co-organised by EDPS

Target	Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017	Result at 31.12.2018
9 initiatives per year	9 initiatives	9 initiatives	9 initiatives	9 initiatives

Number of activities focused on cross-disciplinary policy solutions (internal & external)

Target	Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017	Result at 31.12.2018
8 initiatives per year	9 initiatives	8 initiatives	8 initiatives	8 initiatives

Figure 1. Evolution of KPIs relating to the strategic objective *Data protection goes digital*

Objective 2 - *Forging global partnerships*

Number of initiatives taken regarding international agreements (used in 2015-2016 only)

Result at 31.12.2015	Result at 31.12.2016
3 initiatives	8 initiatives

2015 result was used to set a benchmark, with a target of 5 initiatives set for 2016

Number of cases dealt with at international level (EDPB, CoE, OECD, GPEN, International Conferences) for which EDPS has provided a substantial written contribution

Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017	Result at 31.12.2018
13 cases	18 cases	31 cases	31 cases

2015 result was used to set a benchmark, with a target of 13 cases set for 2016 onwards

Figure 2. Evolution of KPIs relating to the strategic objective *Forging global partnerships*

privacy and data protection and on cross-disciplinary policy solutions. They did not change throughout the mandate, and regularly met their set targets (see Figure 1).

For KPIs referring to the second strategic objective (*Forging global partnerships*), we decided to streamline the monitoring of our work at international level and, in 2017, we changed from two KPIs to one. This meant that contributions on international agreements were monitored together with other contributions at international level. In all cases, we registered results above, or well above, the set target (see Figure 2).

The KPIs referring to the third strategic objective (*Opening a new chapter for EU Data Protection*) covered both supervisory and consultative tasks.

For supervisory tasks, we maintained the same KPI over the whole mandate, on the level of satisfaction of DPOs, data protection coordinators (DPCs) and controllers on cooperation with EDPS and guidance. The results consistently exceeded the set targets, clearly demonstrating the satisfaction of our stakeholders.

For consultative tasks, the relevant KPIs saw a number of changes throughout the mandate. Firstly, the original KPI, on the impact of EDPS Opinions, depended on developments in the legislative process, which made it difficult to stay within the timeframe set for the monitoring of our KPIs. Secondly, the KPI referring to the EDPS inventory of relevant legislative proposals (based on the European Commission's public Work Programme) was affected by changes, both external and internal, in the way in which we performed and monitored our policy advice activities, which also affected our ability to monitor this KPI. However, where measured, the results met or exceeded their targets (see Figure 3).

Objective 3 - *Opening a new chapter for EU Data Protection*

Level of satisfaction of DPO's/DPC's/controllers on cooperation with EDPS and guidance, including satisfaction of data subjects as to training

Target	Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017	Result at 31.12.2018
60% (2015-2017) 70% (2018-2019)	79.5%	88%	92.3%	95%

Analysis of impact of the input of EDPS to the GDPR (used in 2015-2016 only)

Result at 31.12.2015	Result at 31.12.2016
N/A	GDPR: high impact Directive: medium impact

Analysis of impact of the input of EDPS opinions (used in 2017 only)

Result at 31.12.2017
N/A

Level of interest of stakeholders (used in 2018 only)

Target	Result at 31.12.2018
10 consultations	15 consultations

Rate of implementation of cases in the EDPS priority list (as regularly updated) in form of informal comments and formal opinions

Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017	Result at 31.12.2018
83%	93%	100%	N/A

2015 result was used to set a benchmark of 90%

Figure 3. Evolution of KPIs relating to the strategic objective *Opening a new chapter for EU Data Protection*

Some changes also took place with regard to the KPIs relating to the Strategic Enablers (*Communication and management of resources*).

As regards communication activities, between 2017 and 2018 we launched a new website and then implemented changes in the cookie and tracking policy to increase user awareness and be more data-protection friendly. This had an impact on the way we monitored the KPI relating to visits to our website. After analysing our communications activities, we identified results relating to our social media activities as a more meaningful KPI, and will measure this in our KPI results for 2019.

For our KPIs relating to resource management, one - on staff satisfaction - has been monitored on a biennial basis, based on the results of our staff survey. The second KPI, on budget implementation rate, was introduced in 2018 in recognition of the importance of this activity. In both cases, results have matched or surpassed the set targets (see Figure 4).

Enablers – *Communication and management of resources*

Number of visits to the EDPS website (used in 2015-2017)

Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017
195 715	459 370	181 805

2015 result was used to set a benchmark

Number of followers on the EDPS Twitter account (used in 2015-2018)

Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017	Result at 31.12.2018
3 631	6 122	9 407	14 000

Level of Staff satisfaction

Target	Result at 31.12.2015	Result at 31.12.2016	Result at 31.12.2017	Result at 31.12.2018
75%	N/A	75%	N/A	75%

Budget implementation (used in 2018-2019 only)

Target	Result at 31.12.2018
90%	93.8%

Figure 4. Evolution of KPIs relating to the strategic enablers *Communication and management of resources*

4. DATA PROTECTION GOES DIGITAL

The world we live in today is undeniably digital. Technology is developing at an increasingly rapid pace, changing how we live our lives in ways we could never have predicted. Yet, while technological development undoubtedly has its benefits, it is not without risk.

Many new technologies rely on the widespread collection and use of massive amounts of personal data. While technological innovation has raced ahead, institutional reaction has been slow and maintaining control over our own personal data has become increasingly difficult.

Over the past five years, we have made a significant effort to help people take back control. In the EDPS Strategy 2015-2019 we identified an urgent need to consider, and address, the impact of the technological revolution on the rights to privacy and data protection. We called on regulators around the world to take the lead in coordinating an innovative and rapid response to protect fundamental rights and redress the balance. We should all be able to benefit from new technologies without compromising on our fundamental rights. Data protection, we argued, needs to go digital.

The Strategy sets out three action points aimed at developing an effective regulatory approach for the digital era. These focus on the development of privacy-friendly technologies, cooperation with other regulatory bodies and the promotion of a transparent and accountable approach to big data processing. We believe that we have made significant progress in all three areas, establishing the groundwork for data protection authorities (DPAs) and other regulatory bodies to build on over the coming years.

@EU_EDPS

Time for #eudatap to go digital. Technology is not neutral and must not be allowed to dictate ethics #CPDP2015

4.1 Promoting technologies to enhance privacy and data protection

The number of services in all areas of economic and private life using technologies that process personal data in some form is constantly increasing. In many cases, the organisations processing this data do so in order to gain some kind of advantage, be that economic or otherwise. The challenge facing regulators is about ensuring that individuals are protected from the risks these ever-increasing data processing activities entail.

Addressing this challenge means making sure that data protection and privacy measures are properly taken into account for existing and new technological developments. Monitoring and responding to technological challenges, promoting privacy engineering and working with others to establish a common understanding of what should be considered as state of the art in data protection by design are all ways in which the EDPS has contributed in this area.

4.1.1 Privacy engineering

Privacy engineering is an emerging discipline. It focuses on encouraging the development of engineering solutions that protect and enhance privacy and data protection online. Over the past five years, the EDPS has been involved in several privacy engineering initiatives, with the shared aim of integrating data protection and privacy principles into technological development.

The internet privacy engineering network

Under the EU's new data protection legislation, controllers are required to respect the principles

of data protection by design and by default. For technology developers and manufacturers, this means that there is a need to build privacy and data protection into the design and development of technological solutions. To help prepare for these new requirements, the EDPS set up the Internet Privacy Engineering Network (IPEN).

Launched in 2014, IPEN brings together experts from a range of different areas to encourage the development of engineering solutions to privacy problems. Through supporting projects that build privacy into new and existing digital tools, the Network aims to promote and advance state-of-the-art practices in privacy engineering.

Since the first workshop in 2014, IPEN has both grown and evolved. The initial focus of the Network was on exploring the concepts at stake for privacy engineering, clarifying their interpretation and providing a platform to promote available privacy-friendly solutions. Yearly workshops, combined with other meetings, events and panels (see Figure 5), all laid the groundwork for the move to a more targeted approach at the 2019 workshop in Rome.

With new EU rules on data protection now fully applicable, the 2019 workshop focused on establishing a more specific and practical understanding of privacy-friendly technological development. The aim was to reach a common understanding between controllers and developers, regulators and legal experts of what constitutes state-of-the-art technology in data protection by design. It is this common understanding that will help all involved to create new and smart design processes, technologies and business models, which will ensure more effective protection of individuals and their dignity.

Partners in privacy engineering

In addition to working on the IPEN initiative, we have collaborated with other organisations involved in promoting the development of privacy engineering and privacy enhancing technologies. One important partner is the National Institute of Standards and Technology (US-NIST), a branch of the US Department of Commerce, which has established its own Privacy Engineering Program.

We have followed the work carried out by NIST since the launch of their Privacy Engineering Program and have collaborated with them on a range of projects. In addition to attending one of their workshops in 2018, over the past three years we have participated alongside NIST in several privacy engineering events. The EDPS and NIST work in very different legal and institutional environments. However, our approaches to privacy engineering methodologies and objectives share many similarities, which can only be positive for the future development of privacy engineering.

The work NIST produces legally applies only to the US public sector, but data-intensive industries also seem to be taking an increased interest in privacy engineering. The creation of dedicated privacy engineering sections in the relevant industry associations is a good example of this. To help further these initiatives, IPEN has contributed to several relevant events, including conferences organised by the International Association of Privacy Professionals (IAPP) in 2017, 2018 and 2019 and the 2015-2018 editions of the Computers, Privacy and Data Protection (CPDP) conference.

4.1.2 Monitoring and responding to technological developments

It is not only through privacy engineering initiatives that the EDPS has contributed to promoting and raising awareness about the need for privacy-friendly technologies. We also aim to monitor and respond to technological developments, events and incidents, and assess their impact on data protection. This work has resulted in a range of policy papers, Opinions and reports, published over the course of the current mandate.

Developing and sharing technological expertise

Ensuring effective data protection without technological expertise is now impossible. The digital revolution has forced DPAs and other regulators to develop skills in this area. The EDPS has consistently aimed to lead this trend, by sharing helpful analysis of new technological developments.

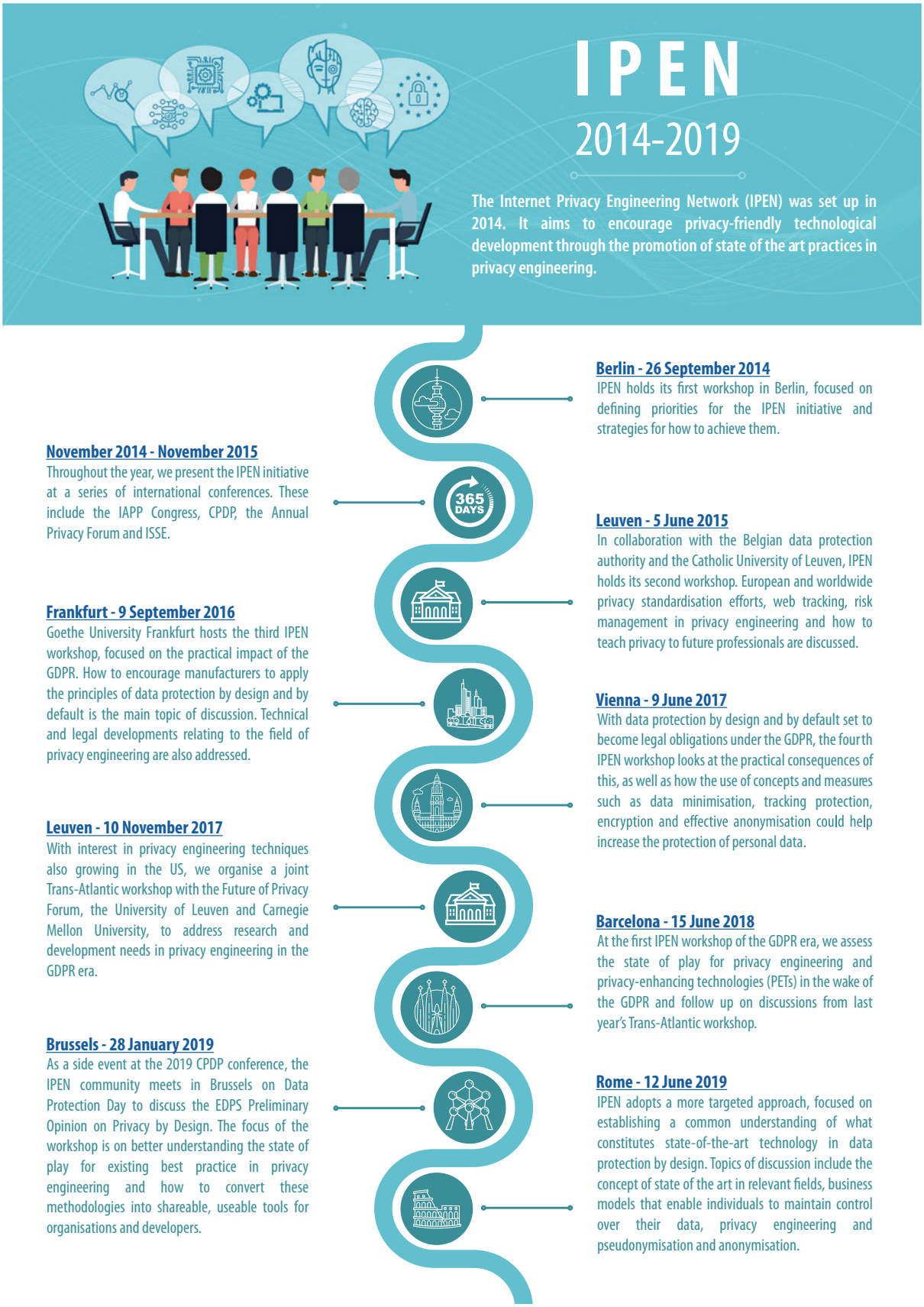


Figure 5. IPEN Workshops, meetings, events and panels, 2015-2019

One example of this is our Technology Monitoring Brief on smart glasses and data protection, published in January 2019. Though smart glasses might seem like something from a science fiction film, they are in fact increasingly available and increasingly used, whether by public authorities, by businesses or by individuals. The interest of law enforcement authorities around the globe illustrates some of the potential of the technology. However, while they may prove useful in a variety of contexts, including technical maintenance, education and construction, smart glasses can have serious implications for privacy, especially when the approach used to develop them does not take into account privacy by design.

Our report on smart glasses explored these implications. It also provided a summary of the cases in which they are currently used and the manufacturers involved, and assessed possible future developments.

Our TechDispatch newsletter is another way in which we hope to contribute. Launched in July 2019, each issue of our TechDispatch aims to explain a different emerging technology. It provides information on the technology itself, a preliminary assessment of the possible impact it could have on privacy and the protection of personal data and links to further reading on the topic.

Another initiative aimed at fostering technological expertise is the EDPS Website Inspection software. In a first for the EDPS, in 2019 we published a software tool to support the work of data protection professionals, such as controllers, data protection officers (DPOs), DPAs and researchers.

Our *Website Evidence Collector* was originally developed to carry out our inspection of EU institutions' websites (see section 6.2.3) and is available for Linux, MacOS X, and Windows. Once set up, and after following a brief introduction, it allows technical amateurs to collect automated evidence of personal data processing, such as cookies or requests to third parties. The collected evidence is documented in a format that is both human- and machine-readable. We published the tool as free software under the EU public licence on the EDPS website and on the code collaboration platform GitHub.

Through publishing information such as this, we aim to contribute to a shared pool of knowledge that all DPAs and other interested parties can benefit from.

Privacy by design

Over the past few years, several scandals involving the misuse of personal data for tracking and profiling have hit the headlines. The ensuing debates have raised a number of questions about the role that technology should play in society. One of these is whether companies ought to be able to use technology exclusively as a means to increase their profits.

Data protection by design and by default are two principles that could help establish human and societal benefit, rather than company profits, as the main driver for technological development. Introduced under the EU's new data protection legislation, these legal obligations require those responsible for collecting and processing personal data to put in place technical and organisational measures to ensure and demonstrate data protection compliance. In the case of data protection by design, this involves planning how to integrate personal data protection into new technological systems and processes throughout a project's lifecycle, while data protection by default involves integrating privacy protection into all technological services and products as a default setting.

On 31 May 2018, just a few days after the EU's General Data Protection Regulation (GDPR) became fully applicable, we published a Preliminary Opinion on Privacy by Design. The Opinion builds on the work of IPEN and the EDPS Ethics Initiative (see section 5.1). It encourages policymakers, regulators, industry, academics and civil society to work together to develop a common approach to technological development, focused on putting human dignity first.

Work to develop this common approach is now underway within various cooperative platforms. These include IPEN, the European Data Protection

Board (EDPB) and the International Working Group on Data Protection and Telecommunications (IWGDPT, also known as the Berlin Group).

Artificial intelligence

There have been some significant developments in the areas of Artificial Intelligence (AI) and robotics in recent years. Yet while new technologies associated with artificial intelligence undoubtedly offer exciting possibilities for the future, they also pose significant challenges for data protection.

AI relies on the use of algorithms, rather than the human mind, to make decisions. This makes it almost impossible for us to access information about how AI technologies process our personal data, as there is no predictable or human decision-making system involved. Providing meaningful consent for the processing of our personal data by these technologies is therefore often impossible.

In 2016, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) identified AI and robotics as one of the main topics of discussion during its closed session, attended by accredited members and observers of the ICDPPC. They wanted to develop a common position on these new technologies. To inform the discussion, the EDPS prepared a background paper, covering what AI and robotics are currently used for and proposing points for reflection.

We returned to the topic at the 2018 International Conference. Here, discussions during the closed session of the conference resulted in an ICDPPC Declaration on ethics and data protection in AI. The Declaration sets out six principles for the future development of AI and demands concerted international efforts to implement these principles. A new permanent working group on Ethics and Data Protection in AI was set up within the ICDPPC to contribute to this effort. The EDPS acts as one of the co-chairs of this group and provides its secretariat.

4.2 Identifying cross-disciplinary policy solutions

Technological development poses a wide range of challenges that DPAs cannot solve alone. Cooperation between regulators, authorities and other experts is necessary if we are to find and implement solutions.

In the digital world, we cannot treat data protection as an isolated area of expertise. We need to work across disciplinary boundaries to address policy issues with a privacy and data protection dimension and develop common, coordinated approaches to the challenges we face.

Over the past five years, we have launched and developed a number of initiatives aimed at increasing cooperation and developing solutions in collaboration with a range of partners. IPEN is a good example of this (see section 4.1.1), but we have also worked with civil society, consumer protection and competition authorities and other regulators in pursuit of shared goals.

@EU_EDPS

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

4.2.1 The digital clearinghouse

There are natural synergies between data protection, consumer protection and competition policy. However, the authorities in these fields have long operated in isolation. If we are to improve understanding of market dynamics and develop coherent and consistent responses to the challenges posed by the digital economy, there is a need for increased cooperation between these authorities.

In September 2016, EDPS Giovanni Buttarelli announced his intention to set up a Digital Clearinghouse. The aim was to promote

The Digital Clearinghouse: 2016-2019

The Digital Clearinghouse was established in 2016 in order to facilitate cooperation between regulators in the fields of data protection, competition and consumer protection.

23 September 2016

The EDPS publishes an Opinion on the coherent enforcement of fundamental rights in the age of big data. In the Opinion, we propose setting up a Digital Clearinghouse, a voluntary network of regulators willing to share information and ideas on how to ensure coherence in the application of the different areas of law relating to the digital economy.

29 September 2016

The EDPS and consumer organsation BEUC host a conference on Big Data: individual rights and smart enforcement. The conference brings together leading regulators in the competition, data protection and consumer protection fields to discuss key areas of global economic and societal change, to promote closer dialogue and cooperation among regulatory and enforcement bodies and to explore how to better respond to the challenges faced by society.

29 May 2017

The Digital Clearinghouse meets for the first time. Regulators discuss common short- and longer-term issues, including data portability, fake news and voter manipulation, the emergence of attention markets and the opacity of the algorithms that determine how personal data is collected and used. Participants start identifying principles for cooperation.

27 November 2017

The Digital Clearinghouse meets for the second time. Discussions focus on several areas in which possible overlaps between domains or gaps in the regulation exist. These include the long-term impact of big technology sector mergers, fake news, security considerations relating to the Internet of Things, harmful or unfair conditions in online platforms and the generation of leads.

21 June 2018

The third meeting of the Digital Clearinghouse is the first to welcome representatives from authorities outside the EU. Topics of discussion include the relevance of personal data in competition and consumer enforcement, the fairness of privacy policies and terms and conditions in free online services, collusive and personalised pricing and related theories of harm in digital markets and unethical data collection and analysis for targeted marketing.

10 December 2018

We expand the scope of the fourth meeting of the Digital Clearinghouse to include electoral regulators. The meeting addresses the impact of online manipulation on free and fair political activities as well as focusing on areas for practical cooperation, such as the deceptive framing of a free offer as unfair practice, asymmetric regulation of access data and the misuse of data protection by national authorities to frustrate investigations.

5 June 2019

At the fifth meeting of the Digital Clearinghouse, the challenges of regulating non-monetary price services are the focus of the morning session. In the afternoon, attention turns to the big tech companies, with a particular focus on recent consumer decisions and actions taken against Facebook.

9 July 2019

In collaboration with the Federal Commissioner for Data Protection and Freedom of Information in Germany, we organise a panel discussion on Data Protection and Competitiveness in the Digital Age. The panel assesses the intersection between data protection and competition policy, in an era in which business models are increasingly reliant on large amounts of personal data.

Figure 6. Digital Clearinghouse meetings and events, 2016-2019

a more coherent enforcement of EU rules on fundamental rights. Made up of a voluntary network of regulators, the Clearinghouse was conceived as a network through which regulators from consumer protection, competition and data protection could share information and discuss how best to enforce rules in the interests of the individual. Endorsed by both the European Parliament and the ICDPPC, our efforts aimed to bring together the various strands of work already underway in this area.

The Digital Clearinghouse met for the first time on 29 May 2017, with all regulators in the digital space, based in the EU or elsewhere, invited to take part in the discussion. The meeting marked the culmination of several years of important discussions on how to respond to the digital challenge and focused on identifying the shared concerns and gaps in regulation that would shape future meetings.

Held twice a year, the focus of the meetings has gradually evolved and the number of participants has grown (see Figure 6). The third meeting was the first to welcome authorities from outside the EU, while the fourth opened up participation to include electoral regulators, to discuss the impact of online manipulation on free and fair political activities, among other topics. With the Clearinghouse well established, the emphasis is now on identifying areas for practical cooperation, on actual cases, in order to ensure that the interests of the individual are at the centre of all new technological developments.

4.2.2 Meeting with civil society

The EDPS, like civil liberties groups, firmly believes that the rights of the individual should be at the core of all EU policy. From the very start of the current mandate, EDPS Giovanni Buttarelli prioritised open dialogue with civil liberties groups as a way to better understand citizens' concerns and ensure they are represented at EU level.

Meetings between civil society groups and the EDPS on the state of data protection and privacy in the EU have taken place regularly since May 2015. The specific focus of our meetings with civil society has changed each year, according to the political climate.

The first meeting took place on 27 May 2015. With the new data protection rules still under discussion, it was an opportunity for us to ensure that the concerns and opinions of civil society were heard and taken into account by the EU legislator. Subsequent meetings have focused on a range of different legislative issues, including the application of the GDPR, ePrivacy reform, Privacy Shield and the monitoring of illegal and harmful content online.

As hosts of the 2018 International Conference of Data Protection and Privacy Commissioners (see section 5.2.1), we also made a conscious effort to ensure that civil society organisations were involved in the public session of the conference, both as participants and as panellists.

On 19 December 2017, in response to a joint statement from the global civil society coalition, we issued an open letter to civil society. The letter reaffirmed the importance of ensuring the active participation of non-governmental civil society representatives, alongside national regulators, academics and representatives from government and industry, in the public session of the conference, in order to ensure meaningful debate. We wanted to create an environment in which a wide range of views could be freely exchanged, and new partnerships built.

In addition to our own initiatives to connect with civil society, the EDPS and the Assistant Supervisor have participated in events organised by civil society groups. These include attending the RightsCon Summit, as well as Assistant Supervisor Wojciech Wiewiórowski providing keynote speeches at both the Freedom not Fear event and the EDRi Anniversary celebration.

4.3 Increasing transparency, user control and accountability in big data processing

Having control over our personal data means being able to determine what data is being

used, for what purpose and by whom. It also means being fully capable of exercising your data protection rights. Yet while this might seem simple in theory, the automated and complex processing of personal data, the use of algorithms to make decisions and the sheer quantity of personal data that is collected, supplemented and shared freely by numerous actors in the modern economy, and particularly online, has made this process considerably harder.

Transparency and accountability in the processing of personal data is now more important than ever before. The EU institutions need to ensure that they set an example for other EU businesses and organisations to follow and it is up to the EDPS, as their data protection supervisory authority, to ensure they do so. Providing training and guidance is one way of doing this (see section 6.2.2), as is undertaking investigations into EU institution activities and exploring solutions that could make accountable and transparent data processing easier.

4.3.1 EDPS investigations

As the supervisory authority for all EU institutions, the EDPS is responsible for enforcing and monitoring their compliance with data protection rules. We are also responsible for ensuring that the public is aware of any possible risks to individual and societal rights and freedoms relating to the processing of personal data. It was in this capacity that, in 2019, we launched two high-profile investigations into EU institutions' compliance with data protection rules.

Communication activities for the EU parliamentary elections

The European Parliament launched several communication initiatives for the 2019 European Union Parliamentary elections. One of these initiatives was to promote engagement through a website called thistimeimvoting.eu, which collected personal data from people interested in the election campaign.

We discovered that the European Parliament was using NationBuilder, a US-based political campaigning company, to deliver services relating to the website. These included the processing of personal data on behalf of the Parliament. Taking into account previous controversy surrounding the company, in February 2019 we opened an investigation into the Parliament's use of NationBuilder, in order to make sure that Parliament's use of the website, and the related processing of personal data, were lawful and compliant with the rules applicable to the EU institutions, set out in Regulation 2018/1725.

The EU parliamentary elections came after a series of electoral controversies both within the EU Member States and abroad. It was therefore of paramount importance that the EDPS intervened, in order to make sure that the Parliament collected and used personal data in a transparent and lawful way. With this in mind, we issued the first ever EDPS reprimand to an EU institution: a contravention by the Parliament of Article 29 of Regulation 2018/1725, involving the selection and approval of sub-processors used by NationBuilder.

We also ordered the Parliament to publish a compliant Privacy Policy. Following their failure to do this before our deadline, we issued a second reprimand.

We plan to check the Parliament's data protection processes in late 2019, once the Parliament has finished informing individuals of their revised intention to retain personal data collected by the website until 2024. We may make further findings once this is complete.

The investigation served as a test of our supervisory role under the new Regulation. As the investigation proceeded, the experience of the European Parliament and the EDPS moved to one of more effective understanding and co-operation, which is vital to secure and protect the interests of EU citizens.

Contractual agreements with external service providers

In April 2019 we launched an investigation into the compliance of contractual and practical arrangements concluded between the EU

institutions and Microsoft relating to the use of Microsoft's products and services.

When relying on third parties to provide services, the EU institutions remain accountable for any data processing carried out on their behalf. They also have a duty to ensure that any contractual arrangements respect the new data protection laws and to identify and take action to reduce and mitigate any risks. This means that contractual terms should include specific organisational and technical measures to protect the privacy and data protection rights of individuals and ensure that, in practice, the processing of their personal data complies with the rules.

The EU institutions rely on Microsoft services and products to carry out their daily activities, which include the processing of large amounts of personal data. The nature, scope, context and purposes of this data processing mean that it is vitally important to ensure that appropriate contractual safeguards and risk-mitigating measures are in place. Our investigation, therefore, focused on identifying the Microsoft products and services used by the EU institutions and assessing whether the contractual agreements concluded between Microsoft and the EU institutions are fully compliant with data protection rules. In addition, we assessed whether the measures agreed with Microsoft, and those implemented by the EU institutions, were appropriate in order to reduce and mitigate the risks posed to individuals and the processing of their personal data by the Microsoft products and services used.

We took a number of different approaches in carrying out the investigation, including on the spot actions to verify facts and practices and to check the measures implemented by the EU institutions. We expect the results of this investigation to help improve the data protection compliance of all EU institutions, but we also want to be at the forefront of positive change outside the EU institutions, to ensure maximum benefit for as many people as possible. Working together with others, we hope to ensure that any necessary product changes and additional contractual and technical safeguards can be used by all public authorities operating in the European Economic Area (EEA).

4.3.2 Personal information management systems

Our online lives currently operate in a provider-centric system, where privacy policies tend to serve the interests of the provider or of a third party, rather than the individual. Using the data they collect, advertising networks, social network providers and other corporate actors are able to build increasingly complete individual profiles, making it difficult for individuals to exercise their rights or manage their personal data online.

While the GDPR and Regulation 2018/1725 provide individuals with increased control over how their personal data is collected and used online, more can and should be done to ensure that individuals are able to take back control of their online identities. The GDPR and Regulation 2018/1725 should be seen as a starting point for the development of a more human-centric approach, based on transparency and user control.

Our September 2016 Opinion on the coherent enforcement of fundamental rights in the age of big data highlighted the difficulties associated with exercising data protection rights in the current digital environment. Our October 2016 Opinion on Personal Information Management Systems (PIMS), however, provided some reasons for optimism. It surveyed efforts to develop a vision of a new reality, in which individuals, rather than online service providers, are able to manage and control their online identities.

The development of PIMS would allow individuals to store their personal data in secure, online storage systems and decide when and with whom to share this information. A variety of designs and business models for this emerging technology exist, but they all share the same idea: to strengthen fundamental rights in the digital world while creating new business opportunities for PIMS providers.

Our Opinion urged the European Commission to support the development of innovative digital tools such as PIMS and to adopt policy initiatives that inspire the development of economically viable business models to facilitate their use. We need to encourage the development of

technological, business and legal initiatives to ensure the effective implementation of data protection rules and help us take back control of our online identities.

The EDPS continues to follow the development of PIMS and other initiatives aimed at increasing transparency and user control. IPEN (see section 4.1.1), for example, is a useful forum through which to monitor these developments.

4.3.3 Online manipulation

On 20 March 2018, we published an Opinion on online manipulation and data protection. With *fake news* and online manipulation both topics of increasing public concern in the months leading up to the application of the GDPR, we argued that the fundamental problem we face is not fake news itself, but the abuse, on a massive scale, of personal information and the right to freedom of expression.

This abuse pervades the entire digital information ecosystem. Over the past two decades, this ecosystem has evolved into an extremely complex structure, controlled by a small number of very powerful technology companies and lacking in accountability. It depends on a cycle of constant tracking, profiling and targeting of individuals, using the information collected to determine what information to present to which people online.

Targeted advertising is one example of how this process works. However, in 2018 it became clear that this ecosystem is being used not only for commercial purposes, but also for political motives, with the aim of disrupting the democratic process and undermining social cohesion.

Opaque algorithmic decision-making is used to determine the content we see online. This process rewards content that provokes outrage, as this inspires greater engagement and therefore generates revenue for the technology company concerned. Such a process poses obvious risks to the protection of fundamental values and democracy.

Our Opinion stressed the need for greater cooperation between regulators in order to ensure that we hold commercial and political players to account for how they process personal data. This means greater cooperation between DPAs themselves, but also increased cooperation across disciplinary boundaries, with roles to play for competition authorities, audio-visual service regulators and those responsible for monitoring elections.

With fears that political campaigns may be capitalising on centralised digital spaces and widely available data to circumvent laws, we turned our attention to a very practical case: the European Parliament elections, which took place in May 2019.

In February 2019, we organised a workshop on how to unmask and fight online manipulation, not only during the EU election, but also during the various national elections due to take place in 2019. The idea was to facilitate a conversation between DPAs, electoral regulators, audio-visual regulators, the media and online platforms and coordinate the fight against online manipulation in elections. The workshop raised awareness of how fake news is generated and spread and included panels addressing the challenges facing democracy, digital vulnerabilities and how regulators from different sectors can work together to combat online manipulation and preserve the integrity of democracy.

On 13 March 2019, the European Data Protection Board (EDPB) adopted a statement on the use of personal data in the course of political campaigns, to which the EDPS actively contributed. Additionally, as part of our supervisory role, we invested considerable effort in monitoring the use of personal data throughout the electoral campaign in the EU institutions, taking action where required (see section 4.3.1).

We aim to ensure that cooperation with all relevant parties continues, both through the Digital Clearinghouse (see section 4.2.1) and through other fora, in an effort to protect democracy and social cohesion worldwide.

5. FORGING GLOBAL PARTNERSHIPS

Data protection laws are set at national or regional level. Personal data, however, flows across borders. Forging global partnerships is therefore vital if we are to ensure the effective protection of individual rights within the EU and elsewhere.

The question of how the data protection community can better engage to achieve greater global convergence in our approach to data protection has long been a topic of discussion. In 2015, the EDPS decided that it was time to move beyond discussion and take action. We wanted to shape a global, digital standard for privacy and data protection, centred on individuals, their rights and freedoms and their personal identity and security. Europe should be at the forefront of this effort, leading by example as a beacon of respect for fundamental rights.

Our Strategy 2015-2019 set out three action points to help us achieve this aim. These involved developing an ethical approach to data protection, ensuring that data protection principles are integrated into all international agreements negotiated by the EU and improving cooperation with our EU allies to promote a coherent and consistent EU approach to data protection on the international stage.

Ensuring accountability in the handling of personal data is a global challenge, but with more and more countries adopting data protection laws, and many of them taking inspiration from the EU's General Data Protection Regulation (GDPR), we can be confident that our efforts are moving in the right direction.

5.1 Developing an ethical dimension to data protection

Over the past few years, social media has become a powerful tool for political and commercial manipulation (see section 4.3.3). Chat bots and automated management have begun to replace human interaction, public surveillance activities have increased, as has public and private sector investment in the development of digital war technology, and the impact of data-intensive technologies on our natural ecosystem has also become a concern.

The digital revolution challenges the traditional frameworks used to ensure respect for our rights to data protection and privacy. There is a real need to question the way in which we use new technologies, to assess the impact they have on our rights and values and determine how to address them.

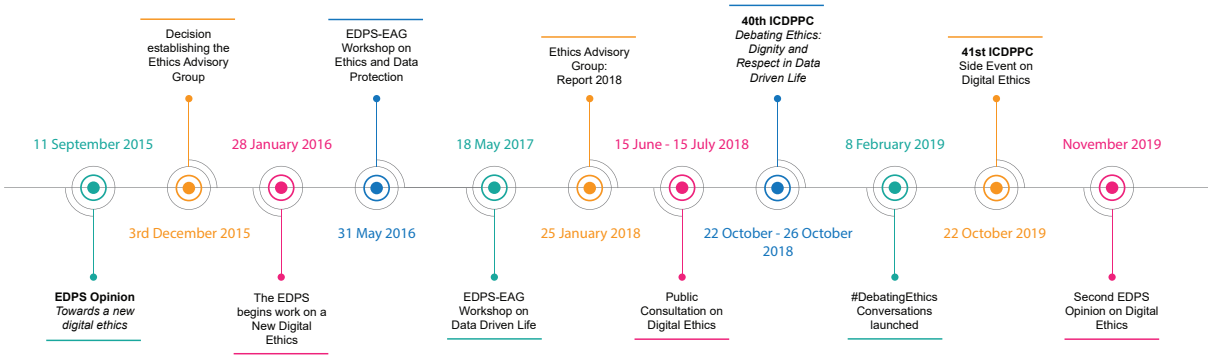
One way in which we could do this is through fostering a continuous debate on what is ethical in the digital sphere. The EDPS invested considerable effort in this endeavour over the course of the mandate. We wanted to launch a global debate on how we can ensure the protection of human rights and fundamental values in the digital age.

5.1.1 The ethics initiative

In 2015, the EDPS launched the Ethics Initiative. This five-year programme, spanning the entirety of the EDPS mandate, aimed to look beyond traditional data protection concerns while exploring the consequences of current and emerging digital technologies on both the individual and society as a whole.

Our aim was to promote awareness and understanding of the risks that we, as a population, currently face. We wanted to assess the links between data protection and privacy and the preservation of human dignity in the digitised world and explore the meaning and importance of these links, taking into account technological developments such as extensive tracking and profiling practices, the Internet of

The EDPS Ethics Initiative:
Three Years in the Making



Things, Big Data, Artificial Intelligence (AI) and autonomous systems, robotics and biometrics.

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

5.1.2 The ethics advisory group

In September 2015 we launched the Ethics Initiative with the publication of an Opinion entitled *Towards a New Digital Ethics: Data, Dignity and Technology*. The Opinion identified technological trends that raise new ethical questions and urged the EU and other international bodies to promote an ethical approach to the development and use of new technologies. We also used the Opinion to declare our intention to create an independent Ethics Advisory Group (EAG).

We announced the members of the EAG at the annual Computers, Privacy and Data Protection (CPDP) conference in January 2016. Made up of six experts from different backgrounds, the EAG was tasked with exploring the relationships between human rights, technology and markets and identifying threats to the rights to data protection and privacy in the digital era.

The group worked together over the course of two years to examine digital ethics from a variety of academic and professional perspectives. The aim of these discussions was to contribute to the wider debate on the digital environment and its ethical implications. During this time, the EAG secretariat, provided by the EDPS, organised two workshops on digital ethics. The first, held in July 2016, explored the relationship between ethics and data protection, while the second, held in July 2017, covered the wider subject of data-driven life.

The work of the EAG concluded in January 2018, with the presentation of their final report at the 2018 CPDP conference. The aim of the report was not to produce definitive answers or articulate new norms, but rather to encourage proactive reflection on what is at stake. It focused on the consequences of the digital revolution and the impact that these consequences have had on the values that we, as individuals and as a society, hold dear.

The EAG identified the core socio-cultural shifts introduced by recent technological change and advised against an instrumental approach to ethics involving ethical checklists, arguing that this approach would put a limit on ethical reflection. It highlighted how new digital technologies pose risks to human autonomy and self-determination

and argued that respect for individual humanity and dignity cannot be preserved in cases where individuals are treated as temporary aggregates of data, processed on an industrial scale in order to enhance, through algorithmic profiling, any type of interaction with them.

@EU_EDPS

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

5.1.3 Debating ethics

With the work of the EAG complete, we turned our attention to encouraging debate on digital ethics around the world. Building on the results of the EAG report, on 15 June 2018 we launched a global public consultation on digital ethics, opening up the debate to contributions from individuals and organisations from all sections of society.

We received 76 responses to the consultation, from a wide variety of sources located all over the world. These included health centres, kindergartens, universities, governments, NGOs, law firms and software developers. The results of the consultation indicated that a clear majority of respondents had embraced an ethics-based approach to data protection, in order to strengthen legal compliance and proactively identify new challenges.

The 40th International Conference of Data Protection and Privacy Commissioners (see section 5.2.1) proved to be a watershed moment for the debate on digital ethics. Hosted by the EDPS in October 2018, we dedicated the public session of the conference to Debating Ethics: Dignity and Respect in Data Driven Life. We wanted to build on the work produced through the EDPS Ethics Initiative to incite a global reaction to the challenges we face in the digital age.

Speakers included activists, academics, representatives from the private sector, presidents of courts, data protection authorities (DPA) and many others from all over the world. Conference participants represented equally diverse backgrounds. We engaged in inspiring debates on the challenges we face in preserving human dignity and respect in today's data-driven societies, but also on how we can address these challenges. Our detailed report on the Conference summarises the main messages of each keynote speaker and panel.

The challenges posed by the digital revolution require a global response. Through the conference, we were able to generate the type of rich, global and cross-disciplinary debate that can inspire us in overcoming these challenges. Our communication efforts throughout the conference enabled us to mobilise a wide range of people, not just within the data protection community and within Europe, but across a wide range of disciplines globally, and make great strides towards achieving a common goal of developing an ethical approach to data protection.

@EU_EDPS

.@Buttarelli_G #GDPR represents an important inspiration worldwide. However, laws are not enough. "Debating #Digital #Ethics" Intl Conference aims at facilitating discussion on how technology is affecting us as individuals and our societies @icdppc2018

5.1.4 Beyond the international conference

It was important to ensure that we capitalised on the progress made at the conference and continued to move the debate on digital ethics forward. Drawing on the issues raised at the conference, we identified several specific areas of concern on which to focus a series of open webinars, which we called #DebatingEthics Conversations.

These *Conversations* allowed us to explore each of the selected topics in more detail, through collaborating with invited experts. They covered themes such as workplace surveillance and the

environmental impact of digital technologies. All episodes are available in the form of podcasts on the EDPS website.

With the #DebatingEthics Conversations complete, in late 2019 we issued a second Opinion on Digital Ethics, highlighting the main concerns identified over the course of the Ethics Initiative and how to move forward.

The International Conference also remains an important forum for discussion in moving the debate forward. The establishment of the ICDPPC working group on Artificial Intelligence, Ethics and Data Protection in 2018 (see sections 4.1.2 and 5.2.1) will ensure that discussion about Digital Ethics remains firmly on the international agenda.

To complement this, we organised a side event at the 2019 edition of the conference, which took place in Tirana, Albania. The event focused on the impact of factors such as global warming and the consequent displacement of large populations and the trend towards the use of biometric and surveillance technology in border management, on our ability to uphold not only the right to privacy, but also human dignity and other fundamental rights and values.

The EDPS Ethics Initiative served as a wake-up call for the data protection community. We succeeded in launching a much-needed debate on values and rights in the digital age that we hope will ensure responsible innovation, with technologies developed in ways that ensure they offer true benefit for society.

5.2 Mainstreaming data protection into international policies

Over the past five years, data protection has really begun to establish itself as part of mainstream public policy. In the digital era, everyone and everything is connected and this connection occurs through the medium of data. In cases where data protection might once have been considered a separate policy issue, it is now a principal policy concern. Discussions surrounding EU trade policy illustrate this well, as

EDPS Giovanni Buttarelli explained in a blogpost published in late 2017.

Throughout the current mandate, we have sought to provide the EU legislator with clear advice on how to coherently and consistently apply EU data protection principles in the negotiation of international agreements involving data flows across borders. We have also closely monitored the implementation of existing international agreements, while stepping up our cooperation with international partners in pursuit of a more coordinated international approach to data protection and privacy.

@EU_EDPS

#Dataprotection should not be subject to #trade negotiations. Read about the relationship between trade & #data in the latest blogpost by @Buttarelli_G: 'Less is sometimes more' http://europa.eu/!YW39rf

5.2.1 The 2018 international conference of data protection and privacy commissioners

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) meets annually with the aim of providing global leadership in data protection and privacy, by connecting the world's data protection and privacy authorities. The EDPS has long been an active participant in the conference and, in October 2018, we had the privilege of hosting the International Conference in Brussels, alongside our co-hosts, the Bulgarian Commission for Personal Data Protection.

The conference began with a two-day closed session, open only to conference-accredited members. We then welcomed participants from all over the world to the public session of the conference. Participants included representatives from government, civil society, regulators, industry, academia and the media, in addition to DPAs. Forty side events on a range of privacy related issues also took place and additional privacy events were organised by our co-host in Sofia, Bulgaria.

The closed session - ethics and artificial intelligence

It is up to the ICDPPC Executive Committee to set the agenda for the closed session of the conference. In 2018, for the first time, however, the central theme of the closed session was directly connected to the theme of the public session.

The closed session of the 2018 conference brought together a record number of delegates, totalling 206 participants from 76 different countries. The topic under discussion was Ethics and Artificial Intelligence.

Few authorities currently monitor the impact of new technologies on fundamental rights so closely and intensively as data protection and privacy authorities. The 2018 conference therefore looked to continue the discussion on AI initiated two years previously, in Marrakesh (see section 4.1.2).

In addition to producing a declaration on ethics and data protection in AI (see section 4.1.2), the closed session adopted three resolutions on e-learning platforms, on the Conference Census and on collaboration between Data Protection Authorities and Consumer Protection Authorities, in addition to a roadmap for the future of the International Conference.

Our hope is that the decisions taken in the closed session will help the conference to grow in ways that will reinforce cooperation globally, both within and outside the data protection community.

The public session - debating ethics

With the choice of topic for the public session at the discretion of the hosts, we chose to focus on *Debating Ethics: Dignity and Respect in Data Driven Life*. We wanted to inspire an inclusive, cross-disciplinary and interactive debate on the digital revolution and its impact on us, as individuals and as a society (see section 5.1.3).

The public session brought together participants from diverse backgrounds and nationalities. These included representatives from the private and public sectors, academia, civil society and the media, as well as guests, members and observers of the ICDPPC. Discussion focused on the notions of right and wrong around the world and across different disciplines, and how these notions underpin law, technology and the way people behave.

The unique theme, programme, format and a range of excellent speakers inspired record attendance levels. This included a record number of NGO delegates. In total, 85 countries were represented, making for a truly international conference.

Press coverage for the conference was also global in scope. Eighty-one media organisations from 23 different countries, including broadcasters, news agencies and leading newspapers, were all active at the conference.

A detailed report on the conference is available on the EDPS website.

@EU_EDPS

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

Side events

Traditionally, side events take place in the margins of the International Conference, and the 2018 conference was no exception. Events focused not only on the conference theme of digital ethics, but also on a wide range of other topics relating to data protection practice. With over 40 events to choose from, there was something for all interests.

Organised by a variety of different organisations and groups from all over the world, the side events that took place during the week of the International Conference provided a unique opportunity for participants to interact with colleagues from diverse disciplines and regions across the world and to learn from their differing perspectives on a wide range of data protection-related issues. Side events were organised by eight different DPAs from around the world, 18 NGOs and international organisations, six think tanks and research groups and eight private companies and law firms. Over 160 speakers were involved.

@EU_EDPS

More than 200 delegates from #DPAs represented at 40th International Conference of #DataProtection & #Privacy Commissioners in Brussels. Warm thank you to more than 1400 delegates, speakers, participants for fruitful discussions & inspiring atmosphere! #DebatingEthics #icdppc2018

5.2.2 Data protection and trade

In early 2018, the European Commission set out the results of the work carried out by its Project Team concerning a stand-alone chapter on cross-border data flows and the protection of personal data, to be included in future trade and investment agreements. According to their proposal, the chapter would consist of two articles, which would cover cross-border data flows and the protection of personal data.

The protection of personal data and privacy are fundamental rights and are therefore not negotiable. This means that, ideally, they should not be included in international trade or investment agreements. Nevertheless, the EDPS welcomed the proposed approach, which strikes a balance between the need to remove barriers to international data flows on the one hand, and the need to preserve EU fundamental rights, including the right to data protection, on the other. We also welcomed the Commission's confirmation that adequacy decisions (see section 5.2.3) should be the preferred legal ground for international data transfers, following a separate data protection negotiation track.

This means that inserting horizontal provisions in trade or investment agreements should only be considered where adequacy is not realistically attainable.

This new approach was applied for the first time in negotiations on the EU and Japan's Economic Partnership Agreement, which entered into force on 1 February 2019. In parallel to these discussions, the Commission adopted an adequacy decision for Japan (see section 5.2.3). The EDPS was actively involved in the European Data Protection Board's (EDPB) discussions on the draft decision in order to ensure a successful outcome under the new approach to data protection and trade agreements.

5.2.3 Evaluating adequacy decisions

The European Commission has the power to decide whether a non-EU country offers a level of data protection that is essentially equivalent to that of the EU, thus allowing for the unimpeded flow of personal data between the EU and the non-EU country in question. These decisions are known as adequacy decisions.

Before adopting an adequacy decision, however, the GDPR and the data protection Directive for the police and justice sectors require the Commission to request an Opinion on their proposal from the EDPB, of which the EDPS is a member.

Over the past five years, we have provided advice to the Commission on two adequacy cases: Japan and the United States.

The EU-Japan adequacy decision

In September 2018, the European Commission published a draft adequacy decision providing for the transfer of personal data from the EU to Japan. Using its updated guidance document on adequacy decisions as a benchmark, the EDPB adopted an Opinion on the draft agreement on 5 December 2018.

As the first adequacy decision of the GDPR era, it was considered vitally important to ensure that the EU-Japan agreement set the highest standard possible. The EDPB wanted to ensure that it set the tone both for future adequacy agreements and for an upcoming review of the adequacy decisions already in place. While the EDPB welcomed the efforts of the European Commission and the Japanese PPC to increase convergence between their respective legal frameworks, it also highlighted a number of concerns, including whether the protection of personal data transferred from the EU to Japan could be guaranteed throughout its full life cycle. The EDPS also provided preliminary informal comments on the proposed adequacy decision on 4 September 2018.

As a member of the EDPB, we actively contributed to discussions on the EDPB Opinion, drawing particular attention to the role of the Board and the accountability of the Commission in the negotiation of adequacy agreements. We were particularly mindful of the importance of ongoing negotiations for the EU and Japan's Economic Partnership Agreement, taking place in parallel, and of the need to ensure that the new European approach to data protection in trade agreements, agreed by the Commission, could be successfully applied in practice (see section 5.2.2).

The Commission modified the draft decision after the EDPB issued its Opinion, and adopted the EU-Japan adequacy decision on 23 January 2019.

@EU_EDPS

Glad #EDPS has strongly contributed to a balanced @EU_EDPB opinion of paramount importance on the first #GDPR adequacy finding: Not a red light, but improvements are recommended to achieve a robust #EU & #Japan #data-protection deal

Safe harbour declared invalid

On 24 March 2015, the EU Court of Justice (CJEU) invited the EDPS to intervene in case C-362/14 Schrems v Data Protection Commissioner, in our capacity as an advisor to the EU institutions on data protection.

The case concerned the Safe Harbour decision, negotiated with the United States government and adopted by the Commission more than 15 years earlier to ensure that personal data transferred from the EU to the US received the same level of protection there as it would in the EU. Though not the only way to transfer data between the two, it was widely used, especially by many of the large American technology companies.

The case stemmed from a complaint relating to transfers of data carried out by Facebook Ireland Ltd. The complainant, a student from Austria, Maximilian Schrems, argued that personal data transferred to the US under the Safe Harbour framework was not adequately protected, drawing on revelations about US mass surveillance to support his argument. As the Irish Data Protection Commissioner considered itself unable to act on the Safe Harbour decision, Schrems took the case to the High Court of Ireland, which referred a number of questions to the CJEU.

In the observations submitted to the CJEU by the EDPS, we made the following points:

- There had long been doubts about Safe Harbour. The Article 29 Working Party (WP29) had previously raised a number of criticisms, but these had never been resolved.
- There was a possibility that the reach and scale of surveillance was so broad that Safe Harbour failed to respect the essence of the fundamental right to privacy and data protection enshrined in the EU Charter of Fundamental Rights.
- Independent data protection authorities have the power to determine what actions are necessary to ensure a fair balance between privacy and the protection of personal data and, in this case, disruption to the internal market.

We concluded that an effective solution to the case would be the negotiation of an international agreement providing adequate protection against indiscriminate surveillance. We specified that this should include obligations on oversight, transparency, redress and data protection rights.

On 6 October 2015, the CJEU declared the Safe Harbour decision invalid. The Court clarified that, when negotiating an adequacy decision for the transfer of data between the EU and a non-EU country, the European Commission must assess both the content of the data protection rules of the country in question and the measures designed to enforce compliance with these rules. This assessment should be carried out periodically to ensure that the situation has not changed.

The Court also ruled that national DPAs must have the authority to examine and challenge the validity of the Commission's adequacy decisions on behalf of any individual who raises concerns.

@EU_EDPS

Careful attention should be given to modalities #international transfers of personal #data in line with #CJEU ruling in @maxschrems #EUdataP

A coordinated approach to the EU-US privacy shield

In early 2016, the European Commission reached a political agreement with the US on a new framework for transfers of personal data. In accordance with procedure, the Commission submitted the agreement, known as the EU-US Privacy Shield, to both the EDPS and the WP29 for consultation.

At the conclusion of their plenary meeting on 2-3 February 2016, the WP29 published a joint statement on the proposal. Their Opinion followed shortly after, on 13 April 2016. Though the Group welcomed a number of significant improvements, compared to the Safe Harbour decision, it also raised some serious concerns about the proposed agreement, noting that some important data protection principles provided for by EU law were missing from the proposal.

The EDPS published our own Opinion on 30 May 2016, building on the recommendations outlined in the WP29 Opinion and reinforcing many of them. Though we welcomed the effort made to develop a suitable replacement for Safe

Harbour, we concluded that the improvements proposed in the new framework were not sufficient. Specifically, we recommended strengthening the main principles of the new self-certification system, including provisions on data retention, purpose limitation and the rights of individuals, and called for strict rules on US public authorities' access to personal data.

The Privacy Shield came into force on 1 August 2016 and a joint review, organised by the WP29, and subsequently by the EDPB, has taken place every year since. The aim of this review is to ensure that the Privacy Shield is implemented in a way that provides for adequate protection of personal data, in line with EU rules. The EDPS has taken part in all reviews to date.

On 28 November 2017, the WP29 published its report on the first annual joint review on the EU-US Privacy Shield, following the publication of the European Commission's report on the first annual review of the functioning of the EU-US Privacy Shield.

The report focused on concerns raised in previous WP29 Opinions relating to the commercial aspects of the Privacy Shield and government access to EU data for the purpose of law enforcement and national security. It recommended that the European Commission and US authorities restart discussions and called for the appointment of an ombudsperson, the clarification of rules of procedure and the filling of vacancies on the US Privacy and Civil Liberties Oversight Board (PCLOB) before 25 May 2018. Any remaining concerns were to be addressed by the date of the second joint review. The report stated that failure to deal with these concerns within the relevant timescales could result in the WP29 taking the Privacy Shield adequacy decision to national courts for them to refer to the CJEU for a preliminary ruling.

The EDPB's report on the second annual review, published on 22 January 2019, acknowledged the progress made in implementing the Privacy Shield, through efforts to adapt the initial certification process, start ex officio oversight and enforcement actions and to publish a number of important documents. The appointment of a new Chair and three new members of the PCLOB, as well as the appointment of a permanent Ombudsperson, were also cited as positive steps forward.

Concerns about the implementation of the Privacy Shield remained, however, particularly in relation to the lack of concrete assurances relating to the indiscriminate collection of personal data and access to personal data for national security purposes. The information provided at the time also failed to demonstrate that the Ombudsperson had sufficient powers to remedy non-compliance. Certain issues raised after the first joint review were also still pending.

The third joint review took place on 12-13 September 2019. A report will follow in due time.

5.2.4 EU-Canada PNR comes under scrutiny

On 25 November 2014, the European Parliament requested an opinion from the CJEU on the compatibility of the draft agreement between the EU and Canada on the transfer and processing of Passenger Name Record (PNR) data with the EU treaties. They also wanted to know if the proposed legal basis for the agreement was appropriate. The European Commission had negotiated this draft agreement as a replacement for the previous arrangement, which expired in 2009.

In 2013, the EDPS issued an Opinion on the draft agreement and, in April 2016, the CJEU invited us to intervene in the hearing. In our pleading to the Court, we made the following points:

- the draft agreement would serve as a benchmark for similar bilateral agreements with non-EU countries put in place in the name of public security and designed to facilitate personal data transfers;
- the guarantees required by Article 8 of the EU Charter of Fundamental Rights need to be respected, including when rules for data transfers are set out in an international agreement;
- judicial scrutiny of EU laws on PNR needs to be strict, as the processing of PNR data is systematic and intrusive and would allow authorities to engage in *predictive policing*.

We concluded that the draft agreement failed to ensure the level of protection required under Article 8 of the Charter.

In its Opinion, published on 26 July 2017, the Court concluded that the EU-Canada PNR agreement was incompatible with Articles 7, 8, 21 and 52(1) of the Charter of Fundamental Rights of the European Union, as it did not preclude the transfer of sensitive data from the European Union to Canada, nor the use and retention of that data. It should have been based jointly on Articles 16(2) and 87(2)(a) of the Charter and several further aspects also needed to be changed in order to ensure compatibility with the Charter.

In particular, there needed to be more clarity on the types of PNR data that could be transferred. The Court noted that passengers should have the right to be notified if their PNR data is processed during or after their stay in Canada and identified a need for an independent supervisory body to oversee the use of PNR data in Canada.

The conclusions reached by the Court represented an important milestone for the EU, setting the standard for any similar agreements between the EU and non-EU countries in the future. The EDPS is closely monitoring developments regarding the ongoing negotiations between the European Commission and Canada and will issue an Opinion once consulted.

5.2.5 Working with international organisations

International organisations are usually not subject to European laws and they benefit from privileges and immunities, which have implications for the applicability of national laws, including data protection rules. However, they are influential advocates for the development of a privacy culture, and often have their own internal rules on the protection of personal data.

To help international organisations in their efforts to develop their own data protection frameworks and provide them with a space in which to share knowledge and experience with one another, the EDPS launched a series of workshops. Originally launched in 2005, we injected new energy into the initiative at the beginning of the mandate.

The fifth EDPS workshop for International Organisations, organised in collaboration with the International Committee of the Red Cross, took place on 5 February 2016, following a hiatus of four years. The workshop has taken place on an annual basis ever since, each one organised in collaboration with a different international organisation (see Figure 7).

The workshops have proved a valuable opportunity for international organisations to share experience and best practice relating to data protection and analyse the common challenges they face. They are also an occasion to assess the state of play with regard to data protection in international organisations.

The size and relevance of the event has grown consistently since 2005. This confirms the need for such a platform, while also demonstrating the increasing awareness among international organisations of the importance of putting in place strong safeguards for personal data. There is a common determination among international organisations to make data protection part of their working culture and to ensure that they are held accountable. The EDPS will continue to lend our full support to this effort.

5.3 Speaking with a single EU voice in the international arena

With one set of data protection rules applicable to all EU countries, the EU should be able to speak with one voice in the international arena. This is not to say that only one person or one organisation should speak on behalf of the EU, but rather that all EU data protection authorities should be consistent proponents of the same approach to data protection, putting the protection of fundamental rights first.

A coordinated EU approach can only strengthen our voice, helping the EU to act as a positive and leading force in shaping a global, digital standard for privacy and data protection. For this to become a reality, effective cooperation and communication between the EDPS and other DPAs in the EU is fundamental. Since 25 May 2018, the EDPB has been the main forum for cooperation between DPAs. Before this, it was

Data Protection within International Organisations

The EDPS works with international organisations through a series of workshops to raise awareness about data protection and to promote the adoption of data protection rules.

First Workshop - Geneva, 13 September 2005

In cooperation with: the Council of Europe and the Organisation for Economic Cooperation and Development (OECD)
On the agenda: The protection of the personal data of staff and others and the processing of sensitive data relating to health, refugee status and criminal convictions.

Second Workshop - Munich, 29 March 2007

In cooperation with: the European Patent Office
On the agenda: The role of the data protection officer, how to establish a data protection regime and cooperating with organisations and countries operating under different data protection standards.

Third Workshop - Florence, 27-28 May 2010

In cooperation with: the European University Institute
On the agenda: The governance of data protection in international organisations, compliance in practice, technological challenges and related security measures in international organisations and the use of biometrics at borders and for internal security.

Fourth Workshop - Brussels, 8-9 November 2012

In cooperation with: The World Customs Organisation (WCO)
On the agenda: the EU data protection reform package, Council of Europe and OECD initiatives on data protection, compliance and transfers of data to third parties, the processing of data about staff, security breach notification procedures and cloud computing.

Fifth Workshop - Geneva, 5 February 2016

In cooperation with: the International Committee of the Red Cross (ICRC)
On the agenda: the state of play of data protection in international organisations, recent developments in data protection and privacy and the impact of these developments on international organisations.

Sixth Workshop - Geneva, 11-12 May 2017

In cooperation with: the International Organisation for Migration (IOM)
On the agenda: 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 and the impact of the GDPR on international data transfers to international organisations.

Seventh Workshop - Copenhagen, 12 July 2018

In cooperation with: the United Nations High Commissioner for Refugees
On the agenda: Privacy standards and oversight mechanisms for international organisations, putting the principle of accountability into practice, international transfers and the legal grounds for processing personal data in the work of international organisations.

Eighth Workshop - Paris, 17-18 June 2019

In cooperation with: the Organisation for Economic Cooperation and Development (OECD)
On the agenda: The challenges posed by the use of web services and social media, contractual arrangements with software providers, personal data transfers to international organisations and the development of risk assessments.

Figure 7. Data Protection within International Organisations workshops

the WP29, the EDPB's predecessor, which laid the foundations for effective cooperation.

5.3.1 Working with our fellow DPAs

Each EU Member State has at least one independent DPA. Some have more than one, depending on the constitutional requirements of the Member State in question. DPAs are the authorities responsible for enforcing and supervising compliance with data protection rules in their respective EU Member States. The role of the EDPS corresponds with that of the Member State DPAs, in that we are responsible for enforcing and supervising compliance with data protection rules in the EU institutions and bodies.

The EU's DPAs and the EDPS work together in a number of different ways to facilitate the consistent and coherent protection of personal data across the entire European Union.

@EU_EDPS

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

The EDPS as an active member of the WP29

The WP29 was established under the GDPR's predecessor, Data Protection Directive 95/46. It served as the main forum for cooperation between the EU DPAs between 1996 and early 2018. From the start of the mandate in 2015 until the establishment of the EDPB in May 2018, the EDPS continued to actively contribute to WP29 activities, coordinating the Key Provisions subgroup, taking part in the WP29's various other subgroups and focusing our efforts where we could add most value. This included WP29 Opinions on the EU-US "Umbrella Agreement", the EU-US Privacy Shield and interoperability.

Much of the WP29's work between 2015 and 2018 focused on preparations for the GDPR and the EDPB, for which the EDPS would provide the secretariat. WP29 cooperation was essential in ensuring that the EU would be able to enforce the GDPR from 25 May 2018 onwards.

The majority of the work relating to these preparations took place within both the Key Provisions subgroup, for which the EDPS acted as coordinator, and the Future of Privacy subgroup, in which the EDPS played an active role. The EDPS assumed the role of co-rapporteur to produce several WP29 guidelines, designed to help businesses and organisations operating in the EU to better understand and implement the requirements of the GDPR.

We also played a part in the WP29's efforts to provide some clarity on the data protection implications of emerging technologies. In particular, the Group looked to interpret and build upon the EU's technology-neutral data protection rules, tackling subjects such as anonymisation, cloud computing and the Internet of Things.

The WP29 needed to ensure that the EDPB and its secretariat were operational from the first day of the GDPR. Practical preparations for this intensified in 2017, with a particular focus on concluding a Memorandum of Understanding (MoU) between the EDPB and the EDPS. The MoU sets out the terms of cooperation between the EDPS and the EDPB. It provides the foundation for our cooperation, ensuring trust, good faith and collegiality between both parties. The EDPS also 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.

Preparations for the GDPR were not the only focus of WP29 work in this period, however. In September 2017, for example, a representative from the EDPS travelled to Washington D.C., as part of the EU delegation that carried out the first joint review of the implementation of the Privacy Shield (see section 5.2.3). This delegation was composed of representatives from the European Commission and several European DPAs. The findings of their joint review were discussed at a WP29 plenary meeting and, on 28 November 2017, the Group issued a report on the Privacy Shield, in which we called for a

number of improvements in the implementation of this agreement.

The EDPB gets to work

Established under the GDPR, the EDPB replaced the WP29 as the forum for cooperation between the EDPS and the DPAs of the EU's Member States on 25 May 2018. It also took on many new tasks, aimed at ensuring the consistent application of the GDPR and the data protection Directive for the police and justice sectors across the EU. The EDPB is an EU body with legal personality and, in certain cases, the ability to adopt binding decisions. The Board can also issue guidelines, recommendations and statements on a wide range of topics.

The supervisory authorities of the EEA EFTA States (Iceland, Liechtenstein and Norway) are also members of the EDPB with regard to GDPR related matters, but they do not have the right to vote or to be elected as Chair or Deputy Chair.

The EDPS is a member of the EDPB, while also being responsible for providing its secretariat. In 2017, we appointed a liaison coordinator, tasked with coordinating all EDPS work relating to the preparation of the EDPB secretariat. This included working with the WP29 to develop the EDPB website and logo (see section 7.1.5), but also to prepare the MoU between the EDPS and the EDPB. EDPS Giovanni Buttarelli and EDPB Chair Andrea Jelinek signed this MoU at the EDPB's first plenary meeting, which took place on 25 May 2018.

As we are a member of the EDPB, EDPS representatives attend and actively contribute to both plenary and subgroup meetings. We continued in our role as coordinator of the Key Provisions Expert Subgroup, and we also act as coordinator in the IT Users Expert Subgroup. Through our active involvement in all subgroups, we contributed to the wide range of EDPB opinions, guidelines and other documents adopted in 2018 and 2019. These included, for instance, the 2018 EDPB Opinion on the draft

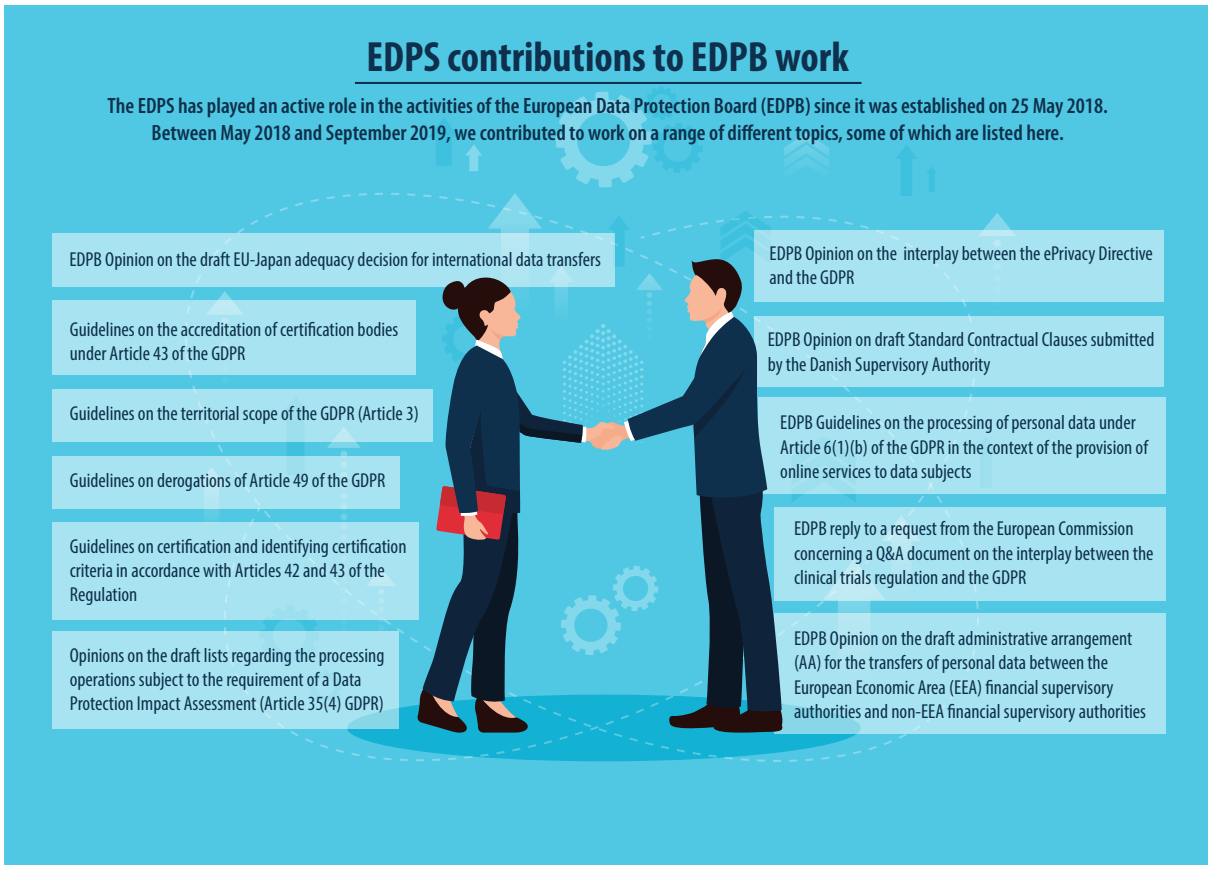


Figure 8. EDPS contributions to EDPB work, May 2018 to September 2019

EU-Japan adequacy decision for international data transfers (see section 5.2.3) and the 2019 EDPB Opinion on draft administrative arrangement (AA) for the transfers of personal data between European Economic Area (EEA) financial supervisory authorities and non-EEA financial supervisory authorities, to which we made significant contributions.

As the number of plenary and subgroup meetings increased in 2019, so did our workload. We have therefore endeavoured to concentrate our efforts on files where our contribution is likely to be most valuable and where the need to present and defend the EU perspective is the greatest (see Figure 8).

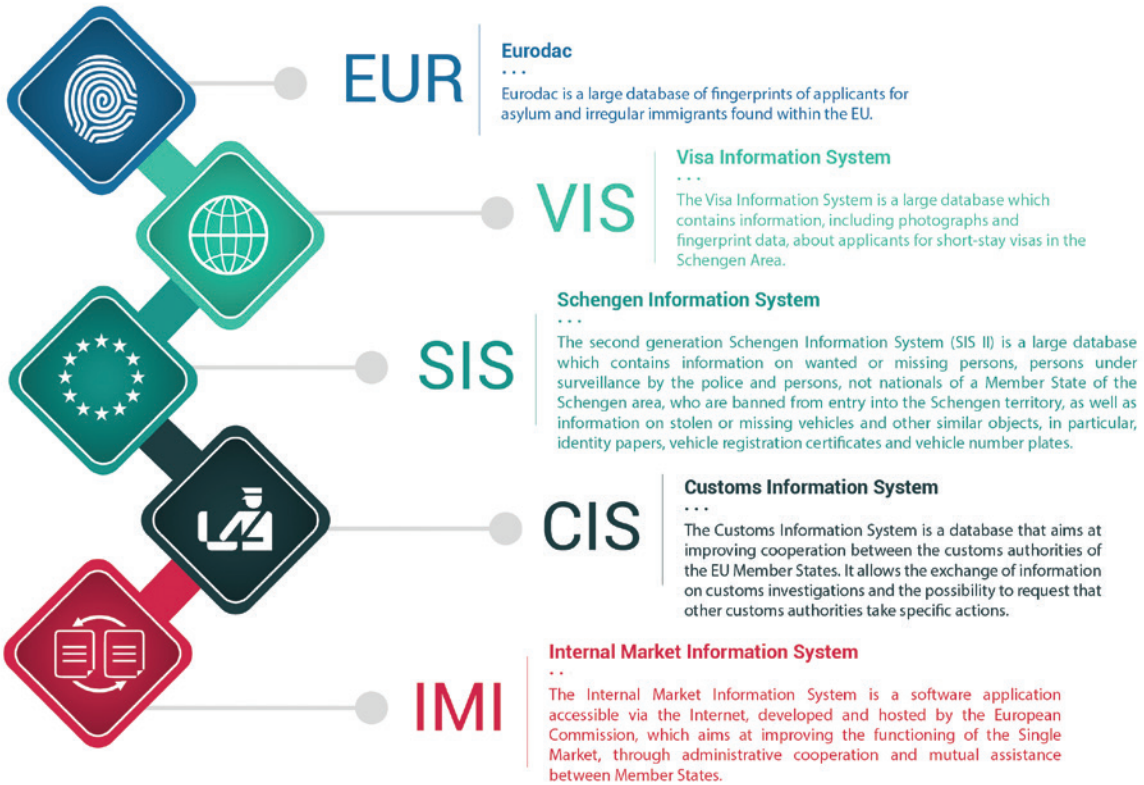
Regulation 2018/1725 provides for the possibility for the Commission to request a Joint Opinion from the EDPS and EDPB in certain circumstances. In July 2019, the first such Joint Opinion was adopted, on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI).

However, joint EDPS-EDPB documents are not limited to consultations under Regulation 2018/1725. We have also issued a joint reply to the European Parliament's Civil Liberties Committee (LIBE), on the impact of the US Cloud Act on the European legal framework for personal data protection.

Coordinated supervision

The EU operates several large-scale IT systems, which are used to support EU policies on asylum, border management, police cooperation and customs. Through the IT systems, national authorities, as well as some EU bodies, are able to exchange information in these EU policy areas.

The EDPS and the national DPAs currently share responsibility for the supervision of these IT systems. While the EDPS supervises the processing of personal data in the central units, the national DPAs are responsible for supervising how their respective national authorities use the IT systems, as well as for the national components of the IT systems.



All supervisory authorities involved, including the EDPS, cooperate through Supervision Coordination Groups (SCGs). Each of these groups is dedicated to a specific EU IT system, with the task of ensuring that supervision efforts on both levels remain consistent.

The EDPS also provides the secretariat for each of the groups, working under the authority of their respective Chairs. The Eurodac, Visa Information System (VIS), Schengen Information System (SIS) and Customs Information System (CIS) groups meet on average twice a year. We publish the results of their meetings on their respective webpages on the EDPS website.

We also engage in activities involving coordinated supervision in our work with Europol. While the EDPS is responsible for supervising the processing of operational personal data by Europol, the national DPAs are responsible for overseeing the processing of personal data by their respective national law enforcement authorities (see section 6.4.3).

As most of the data processed by Europol comes from the national law enforcement authorities, it is essential that we are able to cooperate effectively with the national DPAs in this area. Much of this cooperation takes place within the Europol Cooperation Board, for which the EDPS provides the secretariat. The Board has an advisory function and provides a forum to discuss common issues and develop guidelines and best practice. It meets at least twice a year.

The future of coordinated supervision

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

The new model will not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency, providing for its application, enters into force.

Since 2018, preparatory work has been ongoing within the EDPB to organise this model, currently applicable only to the Internal Market Information system (IMI). The objective is to define practical solutions to put the single model of coordinated supervision envisaged by the legislator into practice. The EDPS continues to play an active role in this process.

To complement the discussion in the EDPB, in January 2019 we organised a panel at the annual Computers, Privacy and Data Protection (CPDP) conference entitled *Checks and balances in the area of freedom security and justice: rethinking governance*. Here, we discussed how we could ensure close collaboration while preserving the independence and role of each oversight body, as well as addressing how to simplify the current supervision schemes.

5.3.2 Closer collaboration with the EU's fundamental rights agency

The EDPS is not the only EU body with a mandate focused on protecting fundamental rights. The EU's Fundamental Rights Agency (FRA) is responsible for providing independent advice on the rights set out in the Charter of Fundamental Rights, which include data protection.

Data protection, privacy and the other fundamental rights and freedoms set out in the Charter are interdependent. On 30 March 2017, EDPS Giovanni Buttarelli and FRA Director Michael O'Flaherty signed a Memorandum of Understanding on increasing cooperation between the two organisations. The document reflects the close and constructive relationship between the EDPS and the FRA, but also represents a commitment to work together to more effectively protect the rights and interests of individuals across the EU.

This commitment was reinforced through collaboration on the revised FRA Handbook on European data protection law, published in May 2018. Alongside the Council of Europe, we co-sponsored the preparation of this Handbook and contributed resources and expertise on EU data protection law and case law.

@EU_EDPS

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

5.3.3 Cooperating with other organisations

In addition to working in close cooperation with our partners in the EEA DPAs, we also work with other organisations and partners with international reach. This kind of collaboration helps to strengthen the united EU voice on the international stage, demonstrating that data protection goes beyond the work of DPAs.

The council of europe

The Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data on 28 January 1981. Known as Convention 108, it was the first legally binding international instrument in the field of data protection.

Any country can sign up to the Convention, with 55 countries now party to the Convention and its additional Protocol regarding supervisory authorities and transborder data flows. This number increases to 70 when combined with the number of countries participating in the Committee of Convention 108 as observers.

The EDPS participates in the Council of Europe's expert groups on data protection, such as the Consultative Committee (T-PD) of Convention 108, as an observer. Our role involves ensuring a high standard of data protection and compatibility with EU data protection standards. The EDPS was also involved in the modernisation of Convention 108, a process that was completed on 18 May 2018.

As of March 2018, the EDPS also represents the International Conference of Data Protection and Privacy Commissioners in the T-PD.

The OECD

The EDPS follows the activities of the Organisation for Economic Cooperation and Development (OECD) Working Party on Security and Privacy in the Digital Economy (SPDE). The OECD is also an active participant in the international organisation workshops organised annually by the EDPS, collaborating with us to host the 2019 edition of this event (see section 5.2.5).

On 1 July 2019, the decision was made to replace the former SPDE with two new expert groups:

- The Working Party on Data Governance and Privacy in the Digital Economy (DGP)
- The Working Party on Security in the Digital Economy (SDE), under the Committee on Digital Economy Policy (CDEP).

The DGP will continue to deal with data protection and privacy matters, while the SDE will focus more on cybersecurity and IT issues, such as cryptography. The EDPS will follow the activities of both groups.

We have also been involved in the work of the OECD Privacy Guidelines Expert Group (PGEG), since its inception at the beginning of 2019. We participated in several preparatory conference calls, as well as in the first PGEG Workshop on accountability held in Paris on 6 May 2019. We will continue to follow the discussions and developments in this group, in cooperation with the European Commission and other participating EU DPAs.

Technological developments

The EDPS also works with various groups at EU and international levels to address the impact of technology on fundamental rights and support the integration of privacy into technological development, including the development of internet structures.

One of these groups is the EU's High Level Internet Group (EU HLIG), composed of representatives from the EU institutions and the Member States. The EDPS participates as an observer. Through the Group, the EU is better able to coordinate its position on certain topics and, therefore, to speak with one voice.

The case of the Internet Corporation for Assigned Names and Numbers (ICANN) is a good example

of this. From 13-15 March 2017, EDPS Giovanni Buttarelli joined representatives from other international data protection organisations to take part in a series of high-level meetings and sessions as part of the 58th meeting of ICANN in Copenhagen. 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 rules and procedures in place at the time provided for uncontrolled access to the personal data of individuals providing resources on the internet and were forcing some providers into conflict with EU data protection rules. By speaking with one EU voice, we were able to convince ICANN to launch a process aimed at adjusting its rules and procedures, to bring them in line with the GDPR.

The EDPS is also a member of the International Working Group on Data Protection and Telecommunications (IWGDPT or Berlin Group). This global body brings together experts from data protection and privacy authorities, academia, civil society and global standardisation organisations. As the debate on the role of technology and its impact on fundamental rights has intensified over the past few years, the work of the Group has taken on increasing importance.

The Berlin Group produces Working Papers, based on an analysis of the technological features involved in the subject under scrutiny. They define principles and recommendations aimed at achieving common objectives. Over the past five years, the Berlin Group has adopted working papers on privacy and security issues in internet telephony, biometrics in online authentication, e-learning platforms, international principles or instruments governing intelligence gathering and data processing and collection in connected vehicles, to which the EDPS has contributed.

In October 2019, the EDPS hosted the Berlin Group meeting in Brussels. The discussions addressed issues such as the new concept of data portability, established by the GDPR, and its possible global impact. With regard to technological developments, the group looked at voice assistants, such as the smart speakers addressed in our first TechDispatch (see section 4.1.2), the growing tracking and profiling ecosystem and developments concerning blockchain technology.

Since 2019, the EDPS has acted as one of the co-Chairs, and provided the secretariat for, the Artificial Intelligence Working Group of the ICDPPC (see section 4.1.2). This working group was created following the adoption of the Declaration on ethics and data protection in Artificial Intelligence, at the 40th ICDPPC in Brussels. The EDPS was one of the authors of the draft Declaration, alongside other members of the ICDPPC.

The EDPS also takes part in the European Dialogue on Internet Governance (EuroDIG) events. This initiative provides a platform for informal discussions on public policy relating to internet governance. It is a forum within which to exchange expertise and best practice, and to identify common ground.

6. OPENING A NEW CHAPTER FOR EU DATA PROTECTION

The EU leads the way when it comes to data protection and privacy standards. Our rules put the individual first, ensuring that each person is able to exercise and benefit from the fundamental rights set out in the EU Charter of Fundamental Rights. However, maintaining this privileged position depends on ensuring that our rules continue to provide adequate protection for individuals in the digital age.

At the beginning of the mandate, the EU was still operating under data protection rules from the pre-digital era. Ensuring that new rules were agreed and put in place as soon as possible was therefore a key aim for the EDPS. We needed to open a new chapter for EU data protection. We needed to develop a new, higher standard for data protection in the digital age that would inspire others around the world to do the same.

In our Strategy 2015-2019 we set out four action points aimed at addressing this issue, the first of these being to support the European Commission, the Parliament and the Council in reaching an agreement on a new EU data protection framework. We also committed to working with the EU institutions and bodies we supervise to ensure that they were prepared for the new rules, to providing advice to facilitate responsible and informed EU policymaking and to helping the EU develop policy approaches that both improve EU security and protect individual privacy.

@EU_EDPS

Our experience as a supervisor gives us knowledge and credibility to advise on the reform of #EUdataP @Buttarelli_G #EDPS

6.1 Adopting and implementing up-to-date data protection rules

In January 2012, the European Commission presented legislative proposals for new EU rules for data protection, designed for the digital age. These rules were to constitute a legislative reform package, covering data protection across the EU, including data protection in the sectors of police and criminal justice.

The reform was the subject of intense and prolonged debate. In our role as an advisor to the EU legislator, we followed the process throughout, providing advice at various stages. With the legislative process still blocked at the beginning of the mandate, we made it one of our priorities to assist the European Parliament, the Council and the Commission in resolving their differences and come to an agreement on a new set of rules. These rules needed to be flexible enough to encourage technological innovation and not impede cross-border data flows, but above all, they needed to empower individuals to more effectively enforce and exercise their rights, both online and offline.

6.1.1 The general data protection regulation

In 2018, we entered a new era in EU data protection. On 25 May 2018, the General Data Protection Regulation (GDPR) became fully applicable to all companies, organisations and institutions operating in the European Union, replacing Data Protection Directive 95/46/EC.

After almost four years of negotiation, the EU legislator came to an agreement on the final text of the GDPR in December 2015. The EDPS followed the process throughout, providing advice to the EU legislator at various stages.

DATA PROTECTION IN THE EUROPEAN UNION

A Timeline

24 October 1995

Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data is adopted

7 December 2000

The Charter of Fundamental Rights of the European Union is published. It sets out the personal, civic, political, economic and social rights of all individuals living in the EU. These include the rights to data protection and privacy

31 October 2003

The EU's Privacy and Electronic Communications (ePrivacy) Directive 2002/58/EC becomes fully applicable across the EU, replacing Directive 97/66/EC

25 November 2009

Directive 2009/136/EC is published, updating the ePrivacy Directive. In particular, it requires that informed consent must be given before a cookie can be installed on a device

25 January 2012

The European Commission proposes a comprehensive reform of the EU's data protection rules, in order to strengthen online privacy rights and boost Europe's digital economy

27 July 2015

The EDPS publishes recommendations on the General Data Protection Regulation (GDPR) and launches a mobile app allowing users to compare the EDPS text against the negotiating texts proposed by the European Commission, the European Parliament and the Council

15 December 1997

Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector is adopted

18 December 2000

Regulation 45/2001/EC comes into force, setting out the rules for data protection in the EU institutions and establishing the EDPS

19 January 2009

Council Framework Decision 2008/977/JHA, applicable to the processing of personal data for police and judicial cooperation in criminal matters, comes into force

1 December 2009

The Treaty of Lisbon enters into force, giving full legal force to the EU Charter of Fundamental Rights. The EU institutions and the EU Member States are now legally required to respect the Charter when implementing EU law

March 2012

The EDPS and the Article 29 Working Party (WP29) adopt Opinions on the European Commission's data protection reform package

28 October 2015

The EDPS publishes recommendations on the Data Protection Directive for the police and criminal justice sectors

15 December 2015

The European Parliament and the Council agree on a text for the GDPR, which sets out the data protection rules applicable to all organisations and businesses operating in the EU, and on a text for the Data Protection Directive for the police and criminal justice sectors

2 February 2016

The WP29 issues an action plan for the implementation of the GDPR

22 July 2016

The EDPS publishes an Opinion on the review of the ePrivacy Directive

10 January 2017

The European Commission proposes two new Regulations, one on ePrivacy and one on data protection in the EU institutions

15 March 2017

The EDPS issues an Opinion on the European Commission's proposal for a new Regulation on data protection in the EU institutions

24 April 2017

The EDPS issues an Opinion on the European Commission's proposal for a Regulation on ePrivacy

6 May 2018

The new Data Protection Directive for the police and criminal justice sectors becomes fully applicable, replacing Framework Decision 2008/977/JHA

22 May 2018

The European Parliament and the Council agree on a text for a new Regulation on data protection in the EU institutions, bringing the rules set out in Regulation 45/2001 in line with the GDPR

25 May 2018

The GDPR becomes fully applicable to all organisations and businesses operating in the EU and the European Data Protection Board (EDPB) starts work

11 December 2018

Regulation 2018/1725 replaces Regulation 45/2001, setting out the rules for data protection in the EU institutions

On 27 July 2015, we published our recommendations on the proposed legislation, to help the EU co-legislators in negotiating the final text. We also launched a mobile app, allowing users to easily compare the texts proposed by the European Commission, the European Parliament and the Council alongside the EDPS recommendations. We wanted to facilitate greater transparency in the negotiation process.

The final text of the GDPR was published in the Official Journal of the European Union on 4 May 2016 and the countdown to when the GDPR would take full effect, on 25 May 2018, began. As part of this process, we updated our mobile app to include the final text of the GDPR.

In addition to strengthening individuals' rights to data protection and privacy, the GDPR strengthened the powers of national data protection authorities (DPAs), giving them the right to advise national parliaments, governments and other institutions and bodies on legislative and administrative measures concerning the protection of personal data. These powers are similar to those that the EDPS has with respect to the EU institutions. Through the Article 29 Working Party (WP29), composed of all EU DPAs and the EDPS, we therefore set to the task of preparing for the GDPR. This included providing guidance on implementing and interpreting the new rules (see section 5.3.1).

Since 25 May 2018, we have continued to contribute fully to efforts to provide advice and guidance on the GDPR, as a member of the European Data Protection Board (EDPB), which replaced the WP29 under the GDPR (see section 5.3.1).

@EU_EDPS

#EDPS app: recommendations support EU to achieve best possible outcome #EUdataP within the boundaries of the 3 texts

6.1.2 The data protection law enforcement directive

In addition to the GDPR, the EU legislator also agreed on new rules for data protection in the areas of police and criminal justice. The Data Protection Law Enforcement Directive ensures that the personal data of individuals involved in criminal proceedings, be it as witnesses, victims, or suspects, is adequately protected. It is also designed to facilitate a smoother exchange of information between Member States' police and judicial authorities, improving cooperation in the fight against terrorism and other serious crime in Europe.

The Directive establishes a comprehensive framework to ensure a high level of data protection while taking into account the specific nature of the police and criminal justice field. It replaces Framework Decision 2008/977/JHA, which previously governed data processing by police and judicial authorities, and covers both cross-border and domestic processing of personal data. It does not cover the activities of the EU institutions, bodies, offices and agencies.

Following the adoption of a general agreement on the new Directive, the EDPS published recommendations on 28 October 2015. We also published a table comparing our recommendations with the proposals put forward for negotiation by the European Parliament and the Council, including them in our mobile app as we did for the GDPR (see section 6.1.1).

The Directive entered into force on 5 May 2016 and Member States had until 6 May 2018 to implement the directive into national law.

@EU_EDPS

#data protection in police & justice sectors should be fully consistent with general rules contained in #GDPR #EUdataP

6.1.3 Setting up the EDPB secretariat

The GDPR also established the EDPB, a new EU body responsible for facilitating cooperation between the EU's national DPAs. The Board took over the responsibilities of the WP29 on 25 May 2018, in addition to many new tasks aimed at ensuring the consistent application of the GDPR across the EU (see section 5.3.1).

Charged with providing the EDPB secretariat, in early 2017 the EDPS appointed a liaison coordinator tasked with coordinating all EDPS work relating to the preparation of the EDPB secretariat. Working under the liaison coordinator, we established an EDPB sector in the second half of 2017, which, on 25 May 2018, became the EDPB secretariat. Their job involves providing administrative and logistical support for the EDPB, as well as carrying out relevant research and analysis tasks.

The EDPS Human Resources, Budget and Administration (HRBA) Unit provides support for the EDPB secretariat. This role included ensuring that the necessary HR infrastructure for the EDPB was in place before 25 May 2018 (see section 7.2.3).

The EDPS was also responsible for preparing the EDPB IT infrastructure. This involved determining the specific requirements of the new IT system for both the EDPB and the individual DPAs and then carrying out a thorough analysis of the technological options available to us. Having identified the most appropriate solution, we were able to ensure that the system was operational by May 2018.

6.1.4 Regulation 2018/1725

The GDPR was not the only landmark event in data protection to occur in 2018. Two days before the launch of the GDPR, the EU legislator reached an agreement on equivalent rules for the EU institutions, bodies and agencies. This legislation, which also defines the role and powers of the EDPS as the supervisory authority for the EU institutions, became fully applicable on 11 December 2018, replacing 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, now set out under Regulation 2018/1725. These rules are equivalent to the GDPR, ensuring that all EU employees and anyone else living in the EU are able to enjoy the same strengthened rights when dealing with the EU institutions as they would under the GDPR.

Although the European Commission's original intention was for the GDPR and Regulation 2018/1725 to apply from the same date, revising the rules set out in Regulation 45/2001 and bringing them in line with the rules set out in the GDPR ultimately took longer than planned.

In 2015, the EDPS set up an informal working group, including a number of data protection officers (DPOs) from the EU institutions, to share views on the revision of the Regulation. In April 2016, this working group submitted a report to the Commission. It compared the provisions of Regulation 45/2001 with those set out in the GDPR and put forward several recommendations for the updated Regulation.

On 10 January 2017, the Commission adopted a proposal for the updated Regulation and we responded on 15 March 2017 with our Opinion. Though we felt that 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 individuals and the need to provide the EU institutions with the possibility to use certification mechanisms in certain contexts. With respect to the tasks and powers of the EDPS, 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.

Discussions on the revised Regulation entered the trilogue phase in November 2017. We responded by calling on the European Parliament, the Commission and the Council to reach an agreement on the new Regulation as quickly as possible, so that the EU institutions could lead by example in the application of new data protection rules. However, it was not until 23 May 2018 that a text was agreed upon. Published in the Official Journal of the European Union on 21 November 2018, Regulation 2018/1725 became fully applicable on 11 December 2018, bringing the rules for the EU institutions in line with the GDPR.

The new Regulation also includes a specific chapter on the processing of operational personal data by EU agencies working in the field of law enforcement and judicial cooperation in

criminal matters, such as Eurojust, which is also subject to its own specific Regulation 2018/1727. These rules are aligned with those set out in the Law Enforcement Directive, which, like the GDPR, became applicable in May 2018.

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

@EU_EDPS

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

6.1.5 ePrivacy

The new rules, in place since 2018, reinforce the EU's position as a global leader in data protection and privacy practice. However, one piece of the regulatory puzzle is still missing. As the GDPR does not regulate the privacy of electronic communications, a new Regulation on ePrivacy, which accurately reflects and supports the principles outlined in the GDPR, is vital to ensuring that individuals' fundamental rights to data protection and privacy are fully respected.

Under the current rules on ePrivacy, traditional electronic communications are subject to clear limitations on the way they use personal data. Companies classified as information society services, however, have flourished due to their ability to exploit loopholes in the current legal framework. There is therefore a clear and urgent need to close these loopholes and strengthen the protection of privacy and the security of online communications.

On 22 July 2016, at the request of the European Commission, we published an Opinion on the review of the ePrivacy Directive, which has been in place in its current form since 2009. In the Opinion, we outlined our position on the key issues relating to the review. We emphasised the need for a new, smarter, clearer and stronger legal framework for ePrivacy and recommended that the scope of this framework be extended, both to match technological and societal changes and to ensure that individuals are afforded the same level of protection for all functionally equivalent services. We also stressed the need to protect confidentiality on all publicly accessible networks and to ensure that user consent, when required, is genuine, free and informed.

On 10 January 2017, the Commission published their proposal for a new ePrivacy Regulation and on 24 April 2017 we issued our response. While we welcomed the proposal, we also set out some of our key concerns. These related to scope and definitions, the need to ensure genuinely freely-given consent, the need for clarity about the relationship between the ePrivacy Regulation and the GDPR and the need to include privacy by default.

On 27 October 2017, the European Parliament responded by approving their Report on the new ePrivacy Regulation. We were pleased to note that this Report followed many of the recommendations provided in our Opinions. It also built 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-rapporteur. Making progress in the Council, however, has proved more challenging.

The scope for negotiation on many points of the proposal is limited, as it would involve compromising on the key principles of communications privacy. Given the importance of ensuring the confidentiality of communications and the particularly sensitive nature of the metadata involved, we urgently need legislation that provides a level of protection equal to that of the GDPR, if not higher.

Despite our best efforts to encourage the co-legislators to move forward with this file, the revision of the ePrivacy legislation was not completed before the European Parliament elections in May 2019. With a new legislative

period now underway, the future of the ePrivacy Regulation is looking increasingly uncertain. The EDPS, however, will continue to push for a satisfactory resolution to ensure that the EU upholds the highest levels of data protection and privacy possible.

@EU_EDPS

#ePrivacy will help fix, not exacerbate, #digital market imbalances through a more consistent and more economically sustainable approach among #EU Member States

6.2 Increasing the accountability of EU bodies collecting, using and storing personal information

In our role as the data protection supervisory authority of the EU institutions and bodies, we are responsible for ensuring that the EU institutions respect the relevant data protection rules. We strongly believe that the EU institutions must lead by example, setting the standard for other organisations and businesses in the EU to follow.

The EDPS has several tools at our disposal to help us to monitor and enforce data protection rules in the EU institutions. These include inspections, visits and the power to deal with complaints. However, we also endeavour to provide the institutions with the tools they need to effectively implement data protection rules, whether this be through regular meetings with DPOs, training sessions with EU management or through the publication of Guidelines. Our focus over the course of the mandate has been on encouraging accountability, ensuring that the EU institutions not only comply with data protection rules, but that they are also able to demonstrate this compliance.

6.2.1 Monitoring and ensuring compliance with regulation 45/2001

Until 11 December 2018, Regulation 45/2001 set out the rules for the processing of personal data in the EU institutions and bodies. It also set out the role and powers granted to the EDPS, as their data protection supervisory authority, to monitor and enforce compliance with the rules. Prior-checks, consultations, inspections and Guidelines are just some of the ways in which we did this.

Prior-checks

Under Regulation 45/2001, all processing operations carried out in the EU institutions likely to present specific risks to the rights and freedoms of individuals by virtue of their nature,

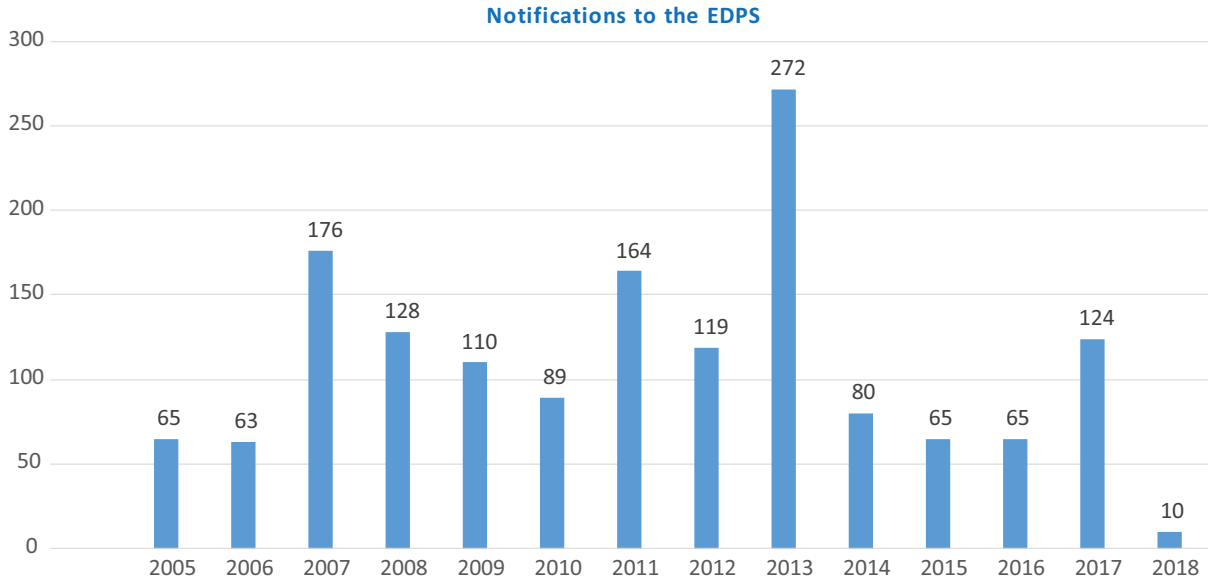


Figure 9. Evolution of Notifications received by EDPS under Regulation 45/2001

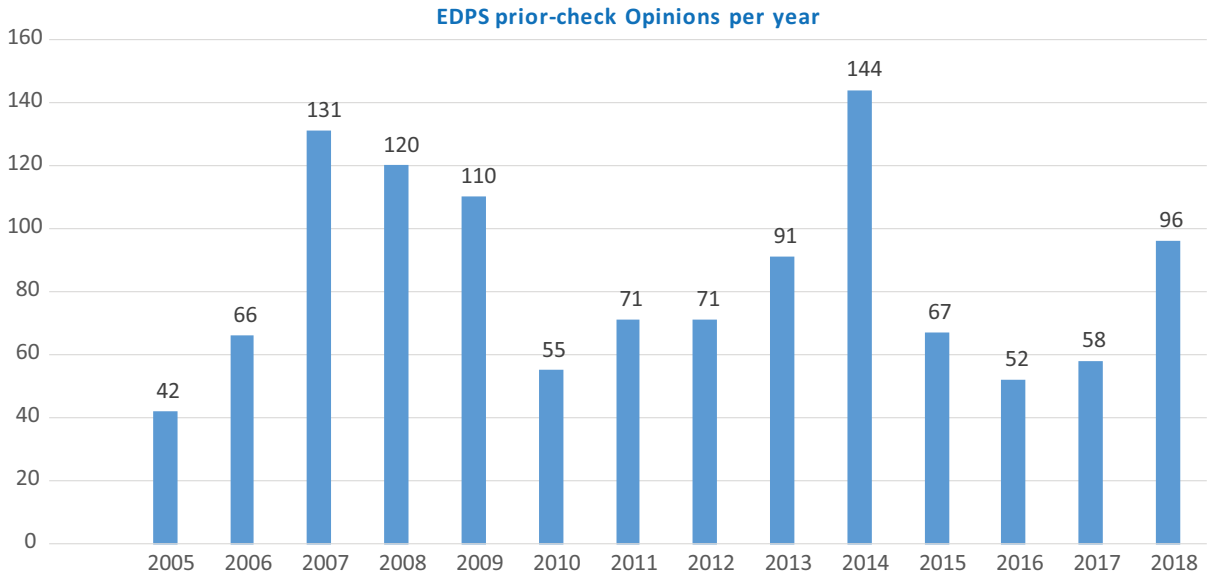


Figure 10. Evolution of prior-check Opinions issued by the EDPS under Regulation 45/2001

their scope or their purposes were subject to prior checking by the EDPS. This involved notifying the EDPS about the proposed processing operation so that we could assess it and provide advice on how to ensure that the procedure complied with data protection rules.

Between 2015 and 2018, when Regulation 45/2001 was in force, we received 267 notifications and issued 298 prior-check Opinions. These dealt with a wide range of issues, from the core business of the EU institutions to administrative processing operations, such as staff management (see Figure 11).

Consultations

Regulation 45/2001 specified that, in certain cases, the EU institutions must request a consultation from the EDPS. EU institutions were also able to consult the EDPS on a voluntary basis, if they had any doubts relating to how to apply the Regulation. These consultations might be formal or informal, depending on the specific circumstances of each case. Consultations were mandatory in the following circumstances:

- if an EU institution was unsure as to whether it was necessary to notify the EDPS for a prior-check opinion, they could refer the case to their DPO who could consult the EDPS for advice.
- when drawing up administrative measures relating to the processing of personal data involving an EU institution.

EU institutions were also able to consult the EDPS on any other matter concerning the processing of personal data. We received 162 such consultations between 2015 and 10 December 2018 and issued 160 responses.

In the same period, we received 29 consultations on the need for prior-checking and issued 30 opinions, while on administrative measures under Regulation 45/2001, we received 20 consultations and issued 21 opinions.

While some consultations were received before 10 December 2018, a response was issued after this date. This explains any discrepancies between the number of consultations received and the number of responses issued.

Complaints

One of the main duties of the EDPS is to hear and investigate complaints and conduct inquiries. This duty remains the same under both Regulation 45/2001 and the new Regulation 2018/1725. Any individual who feels that an EU institution has

Topics for prior-checks, consultations and complaints under Regulation 45/2001

The EU institutions process personal data for a variety of different reasons. Some examples of the topics of prior-checks, consultations and complaints we received under Regulation 45/2001 are listed here.

Prior-checks

Under Regulation 45/2001, all processing operations carried out by the EU institutions that were likely to present specific risks to the rights and freedoms of individuals were subject to prior checking by the EDPS. Examples included:

- social media monitoring by an EU institution
- an EU institution's research into certain medical conditions
- an EU institution's campaign promoting non-discrimination
- whistleblowing in the EU institutions
- due diligence controls on money-laundering and the financing of terrorism
- Confluence - a collaborative space for sharing information about the administrative situation of Accredited Parliamentary Assistants
- the European Aero-Medical Repository

Consultations

In certain cases, Regulation 45/2001 required that the EU institutions request a formal or informal consultation from the EDPS on planned processing operations. Examples included:

- disclosure of personal data by social workers in the EU institutions
- the conditions for sharing data within an EU institution trade union
- the processing of personal data by a national authority using an online tool provided by an EU institution
- the investigative activities of EU institutions, notably regarding anti-fraud, competition and trade
- aligning contractual clauses in service contracts with the conditions specified in the GDPR

Complaints

Regulation 45/2001 required that the EDPS address complaints relating to the unlawful processing of personal data by the EU institutions. Examples of complaints we received included:

- the registration process for an international conference organised by one of the EU institutions
- the protection of privacy and personal data on the websites of certain EU institutions and bodies
- the publication of the name of a candidate who had passed a European Personnel Selection Office (EPSO) competition to become an EU official
- a breach of an EU employee's privacy of correspondence by their employer
- the processing of medical data in disciplinary proceedings and the disclosure of medical data to third parties
- the processing of company data through which an individual can be identified
- a possible breach of the data minimisation principle by one of the EU's Executive Agencies
- access to data in a recruitment procedure at an EU body

Figure 11. Examples of prior-checks, consultations and complaints under Regulation 45/2001

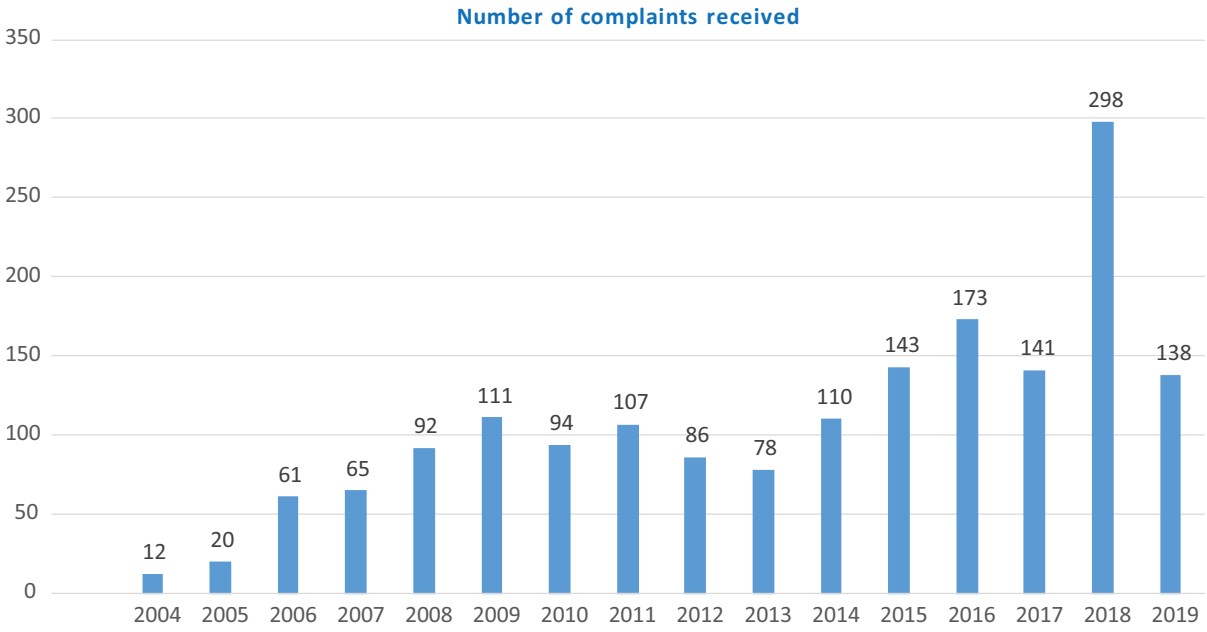


Figure 12. Evolution of the number of complaints, including inadmissible complaints, received by EDPS (up to 31 August 2019).

not respected their data protection rights can submit a complaint to the EDPS.

Between 2015 and 2018 we received 748 complaints relating to a range of different data protection issues. Of these, 573 complaints were dismissed as inadmissible. In most cases, this was because they related to data processing at national level rather than processing by an EU institution or body.

We therefore received 175 admissible complaints and issued 134 complaint decisions in this period. The subjects of these complaints varied from year to year, concerning topics such as the restriction of individuals' rights, the confidentiality and security of processing, the right of access to personal data, recruitment and data transfers (see Figure 12).

Inspections and visits

Inspections and visits are two tools available to the EDPS to help us monitor the EU institutions and ensure that they comply with data protection rules. Visits can also be useful in helping to raise awareness about data protection in the EU institutions.

We carried out 29 inspections and 22 compliance and accountability visits between 2015 and June 2019, at a variety of different EU institutions and bodies. Inspections were used both to ensure compliance with Regulation 45/2001 and, in preparation for the new data protection rules, to ensure that the EU institutions had the right tools to implement an approach to data protection based on accountability. We share the results of our inspections with the institutions concerned and follow up with them in due course to ensure that our recommendations are put into practice.

Compliance visits involve working with the concerned EU institution to draw up a roadmap for compliance. We follow up at a later date to ensure that this roadmap has been effectively implemented. Accountability visits were aimed at preparing the targeted EU institution or body for their transition to the new Regulation.

One of our supervisory responsibilities is to carry out periodic inspections of the central databases of the EU's large-scale IT systems (see section 5.3.1). These inspections focus on the security and management of the systems, while the national authorities are responsible for ensuring the accuracy of the information entered into them. Through carrying out inspections, we are able to monitor data protection compliance, but also to work directly with the EU Agency for the Operational Management of Large-Scale IT systems in the area of freedom, security and

justice (eu-LISA) to approve accountability in the management of these databases.

Inspections and visits continue under Regulation 2018/1725, with a greater focus on encouraging and ensuring an approach to data protection based on increased accountability. This means not only complying with data protection rules, but also being able to demonstrate this compliance.

Spring survey

In 2015 and 2017 we carried out our Spring Survey. This is a periodic review of the progress made by all EU institutions and bodies in implementing EU data protection rules. It allows us to identify any problems and take action to address them.

For each survey, we also identify some specific topics on which to carry out research. These are topics that are considered to be particularly relevant to the work of the EU institutions at the time. In 2015, we focused on international transfers of personal data, information security measures, the effective deletion of personal data and the relationship between the institutions and their DPOs. In 2017 we revisited the topic of international transfers, influenced by recent developments in this area (see section 5.2.3), and also addressed both the collection of identification documents by EU institutions and specific training needs identified by the EU institutions in order to ensure that they were prepared for Regulation 2018/1725.

The results of the two surveys demonstrated that continuous and steady progress had been made in ensuring compliance. The surveys provide us with valuable information that allows us to identify trends and better plan our supervision and enforcement activities.

Cooperation with DPOs under regulation 45/2001

Every EU institution must appoint an independent DPO with the job of ensuring that data protection rules are applied internally. These DPOs meet with the EDPS twice a year, as part of their DPO network meetings (see Figure 13). The meetings serve to reinforce cooperation between the DPOs and ensure that the EU institutions have the necessary tools to lead by example in the application of data protection law.

Between 2015 and 11 December 2018, when the new data protection rules for the EU institutions came into force, DPOs met with the EDPS seven times, hosted each time by a different EU institution, body or agency from across the EU. The first of these meetings to take place under the new mandate was hosted by the European Investment Fund, in Luxembourg. Inspired by the EDPS Strategy, we used this as an opportunity to launch a new and innovative approach to these meetings, focused on making them more dynamic, interactive and efficient, using practical case-studies and interactive workshops.

Armed with the knowledge that accountability would be a key component of the new data protection rules for the EU institutions, our focus was on helping the EU institutions move beyond a purely compliance-based approach to data protection, towards an approach based on being able to demonstrate their compliance. As more details about the new rules were confirmed, we were able to organise our meetings with the DPOs to ensure that they had all the necessary knowledge and tools to help them prepare. Social media and micro-targeting, Data Protection Impact Assessments (DPIAs), IT governance, individuals' rights, data breach notifications and many other topics were all the subject of practical exercises designed to provide DPOs with hands-on experience of how to deal with potential challenges.

To provide further support to DPOs in their preparation for the new rules, on 30 September 2018 we published an updated version of our 2005 position paper on the role of DPOs within the EU institutions. This paper explains their relationship with the EDPS and sets out guidelines on the profile of a DPO and the resources they require to perform their role.

EDPS-DPO meetings 2015-2019

2015

In order to help the EU institutions move from a purely compliance-based approach to data protection to an approach focused on accountability, we launched a new and innovative approach to EDPS-DPO meetings in 2015, focused on interactive workshops.

37th Meeting - 8 May, European Investment Fund (EIF), Luxembourg
Topics of discussion: EDPS Guidelines on mobile devices, accountability, ensuring the security of data processing operations, the role of the DPO in dealing with complaints.

38th Meeting - 5 November, European Union Agency for Network and Information Security (ENISA), Athens
Topics of discussion: dealing with complaints on legal and IT issues, EDPS Guidelines on disciplinary matters, the relationship between information security and data protection.

2016

Meetings in 2016 followed the same format introduced the previous year. Various EDPS Guidelines provided inspiration for many of the activities, with opportunities to put this guidance into practice by applying them to case studies.

39th Meeting - 28 April, Eurofound, Dublin
Topics of discussion: EDPS eCommunications Guidelines, staff appraisals, whistleblowing, cloud computing

40th Meeting - 27 October, European Union Intellectual Property Office (EUIPO), Alicante
Topics of discussion: the right of access to personal data, EDPS Guidelines on mobile apps and web services, Data Protection Impact Assessments (DPIAs)

2017

January 2017 saw the publication of a proposal on new data protection rules for the EU institutions. With a clearer idea of what the new rules would entail, the 2017 meetings focused on providing DPOs with the relevant knowledge and tools to lead by example in applying these rules.

41st Meeting - 1 June, European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), Tallinn
Topics of discussion: DPIAs, accountability, individuals' rights under the EU's new data protection rules

42nd Meeting - 13 October, European Medicines Agency (EMA), London
Topics of discussion: DPIAs, accountability, data breach notifications

2018

Just a week before our first meeting of the year, a political agreement on the new Regulation for data protection in the EU institutions was reached. With the new rules set to apply from late 2018 onwards, our first meeting focused on ensuring that the EU institutions were ready to put these rules into practice. The second meeting, held the day after these new rules came into force, provided an opportunity for DPOs to reflect on the new challenges facing them.

43rd Meeting - 31 May, EDPS, Brussels
Topics of discussion: social media monitoring, data protection records, DPIAs, IT governance

44th Meeting - 12 December, European Parliament and EDPS, Brussels
Topics of discussion: internal rules, the data breach notification procedure, joint controllership, the protection of personal data processed by the EU institutions' web services

2019

With the new rules now in place, 2019's meetings provided us with a chance to take stock of the challenges faced by DPOs in applying these rules, and to find ways to overcome them.

45th Meeting - 17 May, European Insurance and Occupational Pensions Authority (EIOPA), Frankfurt
Topics of discussion: event organisation, data breach notifications, joint controllership, procurement, the obligations of the controller and the processer

46th Meeting - 7 November, Historical Archives of the EU (HAEU), Florence
Topics of discussion: recent case law, archives, contracts with software providers

Figure 13. EDPS-DPO meetings 2015-2019

Thematic guidelines

The EDPS publishes Guidelines on a range of subjects common to many of the EU institutions, such as recruitment, appraisals, the use of IT equipment in the workplace and disciplinary procedures. These Guidelines consolidate the guidance provided in our prior-check Opinions and consultations, as well as guidance issued by the WP29 and in the case law of the European Courts. Many of our Guidelines can also be used as a source of inspiration for organisations other than the EU institutions or to supplement the guidance offered by national DPAs.

Over the course of the mandate we issued 17 sets of Guidelines (see Figure 14). Though the vast majority of these Guidelines were published before Regulation 2018/1725 entered into force, they are still relevant today, as the main principles have not changed. Guidelines issued since the publication of the proposal that became Regulation 2018/1725 were written with the new rules in mind.

Many of the Guidelines relate to developments in IT. These include our Guidelines on IT governance and IT management, the use of cloud computing by the EU institutions and bodies and on the protection of personal data processed through web services provided by the EU institutions (see section 6.2.3). Other examples include Guidelines on whistleblowing, administrative inquiries and disciplinary procedures and documenting processing operations (see Figure 14).

6.2.2 Facilitating the transition to regulation 2018/1725

Regulation 2018/1725 replaced Regulation 45/2001 on 11 December 2018. Like Regulation 45/2001, it sets out the rules for data protection in the EU institutions and the role and powers of the EDPS, bringing them in line with the rules set out in the GDPR.

As the data protection supervisory authority for the EU institutions, our responsibilities extended not only to enforcing the new rules once they were in place, but also to helping the EU institutions prepare for the new rules.

Ensuring accountability on the ground

The GDPR and Regulation 2018/1725 both stress the importance of accountability. This is the idea that the data controller, the organisation responsible for processing personal data, must not only comply with data protection rules, but also be able to demonstrate this compliance.

In order to make accountability a reality, all EU institutions, just like other organisations operating in the EU, must ensure that they adequately document their data processing activities. To help with this, we issued an accountability on the ground toolkit.

A preliminary version of the toolkit was published in February 2018, in order to help the EU institutions in their preparations for the new rules. We updated it to accurately reflect the final version of Regulation 2018/1725 and have further improved the text on several occasions since. The most recent version was published on 16 July 2019. It provides guidance on how to document a processing operation, through what are known as records, and also sets out the criteria for determining when a DPIA is required.

The toolkit complements our work on accountability with DPOs, as well as the training sessions and accountability visits carried out over the course of the mandate.

One of the areas in which Regulation 2018/1725, like the GDPR, introduced significant changes, is in the rules governing the outsourcing of the processing of personal data. Under the new rules, contractors now have a direct responsibility to ensure compliance.

However, when relying on third parties to provide services, the EU institutions, just like any other data controller, remain accountable for any data processing carried out on their behalf. It is the controller's responsibility to use only those contractors that meet the requirements of the applicable data protection law.

To help the EU institutions with this, the EDPS adopted Standard Contractual Clauses for processors in December 2018. These set out the

EDPS GUIDELINES 2015-2019

EDPS Guidelines address a range of subjects common to many of the EU institutions. They provide EU staff members with practical advice on how to ensure compliance with data protection rules.

December 2019 - **Proportionality of measures that limit the fundamental rights to privacy and data protection**

Policymakers need to be able to demonstrate that any proposed measure that would limit fundamental rights is proportional, taking into account the policy aims and purpose of the data processing operation proposed. These Guidelines help policymakers to evaluate the proportionality of any new measure and adjust their proposal accordingly.

17 July 2019 - **Data Protection Impact Assessment List**

DPIAs were introduced under both the GDPR and Regulation 2018/1725 for the EU institutions to ensure that controllers adequately address privacy and data protection risks in certain high-risk processing operations. The EDPS DPIA list can be used to help determine the cases in which it is necessary to carry out a DPIA.

20 December 2018 - **Article 25 of Regulation 2018/1725**

The restriction of data protection rights is only possible in exceptional circumstances. Any restriction must be based on a legal act or on internal rules. Our Guidelines focus on the conditions under which internal rules may be used to restrict data protection rights, how to write internal rules and how to interpret and apply restrictions in practice.

23 March 2018 - **IT governance and IT management**

Under the GDPR, organisations responsible for processing personal data must ensure that they put in place effective risk management policies to protect the fundamental rights and freedoms of the individuals concerned. This includes managing IT security risks, which these Guidelines address.

November 2019 - **Concepts of controller, processor and joint controllership**

The concepts of controller, processor and joint controllership refer to the different roles that entities may assume when carrying out specific processing operations. Our Guidelines help EU institutions and bodies to identify their role and to determine their responsibilities and the steps to be taken to ensure best data protection practice.

16 July 2019 - **Accountability on the ground**

The GDPR and Regulation 2018/1725 both stress the importance of accountability. This is the idea that organisations must not only comply with data protection rules, but also be able to demonstrate compliance. This toolkit is designed to ensure that the EU institutions put accountability into practice, by helping them to adequately document their data processing activities.

7 December 2018 - **Personal Data Breach Notification**

Under the new data protection rules, all EU institutions have a duty to report certain types of personal data breaches to the EDPS. This means ensuring that they have prevention and detection mechanisms in place, as well as investigation and internal reporting procedures. These Guidelines provide the necessary practical advice and information to help them do this.

16 March 2018 - **The use of cloud computing services**

Cloud computing has become an increasingly appealing tool for many EU institutions, but it raises many complex issues for data protection. Our Guidelines provide practical advice and instructions on how to assess and manage the risks to data protection, privacy and other fundamental rights posed by the processing of personal data by cloud-based services.

15 January 2018 - Transparency rights and obligations

All members of EU institution staff responsible for processing personal data on behalf of their institution must put the new data protection rules into practice. These Guidelines help them to get started in fulfilling their new obligations, focusing on how to provide transparent information in the form of a data protection statement.

18 November 2016 - Administrative inquiries and disciplinary procedures

All EU staff must abide by the Staff Regulations. However, though these Regulations help to identify when someone has broken the rules, they do not specify how the EU institutions should deal with rule-breakers. Our Guidelines address this issue, providing the EU institutions with a framework by which to conduct administrative inquiries and disciplinary procedures in line with data protection rules.

7 November 2016 - Web Services

The EU institutions and other organisations are increasingly reliant on online tools to communicate and interact with citizens. With online transactions becoming more and more complex, effective data protection policies are needed to protect the rights of users. This is particularly important in relation to cookies, online tracking, security and personal data transfers, as these Guidelines demonstrate.

17 December 2015 - Mobile Devices

With mobile devices becoming increasingly common in the daily work of the EU institutions and other organisations, we published Guidelines providing practical advice on how to integrate data protection principles into the management of mobile devices in the workplace.

11 April 2017 - Necessity Toolkit

As part of our commitment to facilitating responsible and informed policymaking, the EDPS published a Necessity Toolkit. The toolkit is designed to help policymakers identify the impact of new laws on the fundamental right to data protection and determine the cases in which the limitation of this right is truly necessary.

7 November 2016 - Mobile Applications

Most mobile apps are designed to interact in a specific way with a wide range of online resources and to exchange information with other connected devices. This often involves the collection of great quantities of personal data. In our Guidelines, we provide advice on how to ensure that mobile apps process this data in a privacy-friendly way.

18 July 2016 - Whistleblowing Procedures

Confidentiality is the most effective incentive to encourage staff to report wrongdoing at work. Our advice on whistleblowing procedures aims to ensure that EU institutions are able to provide safe channels for EU staff or other informants to report fraud, corruption or other serious wrongdoing in organisations.

21 March 2016 - Security measures for personal data processing

Different organisations face different security risks relating to the information they use. Our Guidance provides EU institutions with advice on how to create and maintain a secure and trustworthy digital environment for information that is essential for the functioning of their services.

16 December 2015 - Electronic Communications

In most organisations, including the EU institutions, electronic communications are now essential. These EDPS Guidelines provide the EU institutions with practical advice and instructions on the processing of personal data by eCommunications tools, to ensure they remain compliant with the relevant data protection legislation.

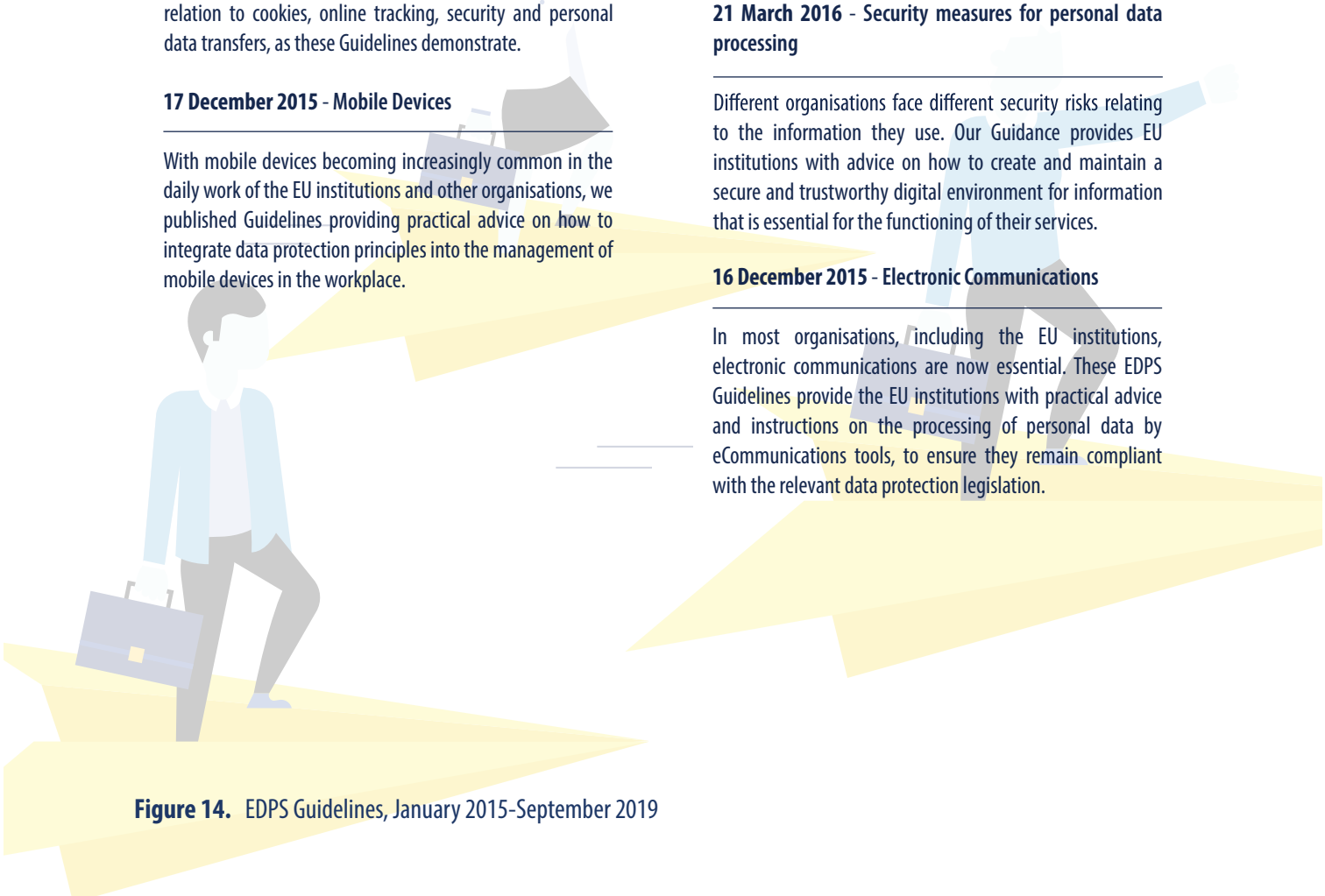


Figure 14. EDPS Guidelines, January 2015-September 2019

minimum requirements for EU institutions for the outsourcing of processing of personal data.

Training sessions and accountability visits

In anticipation of Regulation 2018/1725, we worked closely with DPOs and other representatives from all EU institutions, bodies and agencies throughout 2017 and 2018 to ensure that they were prepared. Activities included interactive workshops organised as part of our twice-yearly meetings with DPOs (see sections 6.2.1 and 6.2.2), as well as accountability visits, training sessions and conferences. We wanted to ensure that all EU staff involved in the processing of personal data, regardless of their position in the EU hierarchy, were aware of the new rules and their implications.

Our awareness-raising campaign intensified in 2018, to ensure that the EU institutions had the necessary knowledge and tools to apply the new rules with ease when they came into force at the end of that year. The campaign put particular emphasis on the importance of accountability, the idea that EU institutions not only comply with data protection rules, but that they are also able to demonstrate this compliance.

One of the key components of our awareness campaign was our programme of training sessions and visits. Designed to reinforce our written guidance (see section 6.2.1), these included a visit to EU institutions and bodies in Luxembourg by Assistant Supervisor Wojciech Wiewiórowski, training sessions for the EU institutions in Luxembourg and for staff at the EU agencies in Athens, an exchange with communication officers from the EU institutions and a training session for staff working for the EU agencies in Italy, as well as numerous bilateral and other meetings with top management in the EU institutions.

Our programme of visits and training sessions continued into 2019. With the new rules in place, it is more important than ever to ensure that all EU staff members responsible for processing personal data are aware of their new obligations and how to put them into practice. A dedicated training session on procurement for case officers at the European Parliament's Directorate General for Finance and an opportunity to engage with the European Commission's Directorate General for Human Resources (DG HR), one of the sectors most heavily impacted by the new rules, are good examples of our continued efforts to facilitate the transition to the new rules.

@EU_EDPS

#EDPS training on new #dataprotection regulation for #EUinstitutions addressed to high-level management at @Europarl_EN - @W_Wiewiorowski stresses the importance of #transparency of operations and #accountability in the heart of #EU #democracy

Cooperation with DPOs under regulation 2018/1725

On 12 December 2018, just a day after Regulation 2018/1725 came into force, DPOs gathered in Brussels for the 44th EDPS-DPO meeting (see Figure 13). It provided a chance for us to reflect on the challenges faced by the EDPS and DPOs under the new legislation.

The day's activities were planned around a series of case studies aimed at providing DPOs with hands-on experience of how to deal with some of these challenges. These included the restriction of individuals' rights, data breach notifications and joint controllership. Our aim was to encourage DPOs to see the rules as a reference tool on how to ensure respect for the rights of individuals, rather than a burden.

A further meeting took place in May 2019. This was an opportunity to take stock of the challenges that DPOs had encountered in applying the new rules and how to overcome them. We were also able to present our strategy for monitoring the application of Regulation 2018/1725 to DPOs.

With the new rules in place, constructive cooperation with DPOs is now more important than ever if we are to ensure that the EU

EDPS Training 2018

Brussels - 31 January

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

Brussels - 16 February (and more)

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

Lisbon - 25 May

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

Brussels - 7 June

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

Maastricht - 26 June

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

Luxembourg - 30-31 January

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

Athens - 1-2 March

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

Brussels - 29 May

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

Brussels - 14 June

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

Stockholm - 18 September

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

Luxembourg - 1-2 October

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

Brussels - 7 November

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

Brussels - 20 November

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

Paris - 26 November

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

Turin - 20-21 September

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

Brussels - 23 October

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

Frankfurt - 12 November

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

Brussels - 21 November

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

Brussels - 3 December

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

institutions are able to lead by example in data protection practice.

@EU_EDPS

.@W_Wiewiorowski stressed the essential role of the #DPO network is ensuring the protection of fundamental rights of individuals. It's about people, not #data. As a result of their close cooperation with the controllers, they will prevent sanctions.

Knowledge management

The EDPS celebrated its fifteenth birthday in 2019. Much has changed since our small institution was set up back in 2004 and, over the past few years, the need to consolidate our knowledge and work in one, easily-accessible place, so that we are not overly reliant on individuals for expertise, has become increasingly evident. This would also allow us to strengthen our position as a provider of expert knowledge on data protection, particularly when it comes to raising awareness within the EU institutions and providing advice on risks, rights and obligations under Regulation 2018/1725.

To address this, in 2018 we launched several activities related to knowledge management. One of the main activities was the creation of an internal Wiki on the new Regulation. The idea was to encourage colleagues to share their knowledge in the creation of an annotated version of the new law, which would help us to ensure a consistent approach to supervising and enforcing data protection in the EU institutions.

To build on this collaborative approach, we organised internal workshops for colleagues to share their specific skills and knowledge and to discuss new concepts and important case law. These workshops help us keep abreast of new developments that might have an impact on our supervisory work. They should also prove useful in helping us to promote public awareness and understanding of the risks posed by certain new technologies to individuals' rights and freedoms and to society. One set of workshops focused on digital ethics, for example. This allowed us to look beyond our immediate day-to-day work and better understand the broader societal impact of technologies.

6.2.3 Protecting personal data in a digital world

Putting the new rules into practice requires that the top management of each EU institution set the tone by integrating data protection into risk management plans and ensuring that data protection is ingrained into the culture of their institution. This has taken on increased importance in the digital era.

To help, we provided guidance and training on a variety of topics such as accountability (see section 6.2.2), risk assessment and DPIAs and data breach notifications, all of which are new and unfamiliar topics for the EU institutions. In addition, we have invested in the development of more sophisticated tools for inspecting IT systems and websites, helping us to monitor the application of the new rules to digital technologies more effectively.

Inspecting IT systems and websites

One of our tasks as the supervisor of the EU institutions is to carry out inspections of the EU's large-scale IT systems, in addition to the activities of the EU institutions themselves (see section 6.2.1). With the IT tools used by the EU institutions becoming increasingly sophisticated and the number of EU IT systems set to increase, we identified a need to improve our methodology and capabilities for inspections.

With the IT Policy lab up and running, in July 2018 we began a programme of remote inspections on the web services offered by the EU institutions. Having published Guidelines in November 2016 on the protection of personal data processed through web services provided by EU institutions, the remote inspections were to serve as a follow-up exercise.

To carry out the inspections, we developed a number of specialised software tools. This included our website evidence collector, which automatically collects information on personal

data processing by websites, such as the use of cookies, web beacons, page elements loaded from third parties and the security of encrypted connections (HTTPS). This tool is now available on the EDPS website under a free software licence, meaning that anyone can download and use it (see section 4.1.2).

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

The results of the first inspection revealed that several of the websites inspected were not compliant with Regulation 2018/1725, nor with the ePrivacy Directive, and did not follow our Guidelines on web services. One of the issues encountered was third-party tracking without prior consent, which is particularly problematic in cases where the third-party concerned operates under a business model based on the profiling and subsequent behavioural targeting of website visitors. Other issues included the use of trackers for web analytics without visitors' prior consent and the submission of personal data collected through web forms using non-encrypted connections.

The institutions inspected reacted swiftly to start rectifying the problems we identified. All those concerned now provide secure HTTPS connections and have significantly reduced the number of third-party trackers they use. We plan to follow up on their efforts while continuing with further waves of inspections.

We continue to invest in the EDPS IT Policy lab. A public procurement procedure is currently ongoing in order to update the capacity of the lab. This will allow us to also carry out remote inspections of mobile apps.

Personal data breaches

Under Regulation 1725/2018 all European institutions and bodies have a duty to report certain types of personal data breaches to the EDPS. Every EU institution must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to pose a high risk of adversely affecting individuals' rights and freedoms, the EU institution must also inform the individuals concerned without unnecessary delay.

Up until 30 September 2019, we had received and assessed 65 personal data breach notifications under Regulation 2018/1725.

On 4 April 2019 we organised a conference in partnership with the European Union Agency for Network and Information Security (ENISA). The event addressed the assessment of risk in personal data breaches. Our focus was on the challenges surrounding risk assessment, examining the legal obligations set out in the GDPR and Regulation 2018/1725.

Risk assessment is a core element in preventing and responding to personal data breaches, which inherently create a lot of uncertainty. Unlike other traditional risk assessment methodologies, the focus in a personal data breach is on evaluating the risk to the rights and freedoms of individuals. While various stakeholders, supervisory authorities and private and public organisations use a range of different methodologies to do this, our data breach Guidelines aim to simplify the task by providing practical examples to assist the EU institutions in their efforts.

In addition to this conference, we worked with the European Commission to organise several data breach workshops. We developed specific training material in cooperation with the Commission and provided our guidance on key issues related to the personal data breaches. Two workshops took place, on 14 and 21 June 2019, with more than 100 participants from a wide

@EU_EDPS

#EDPS @enisa_eu kick off now their joint conference towards assessing the risk in personal #databreaches #CyberSecurity #GDPR #DataProtection

range of the European Commission's different Directorate Generals.

Cloud computing

Cloud computing has become an increasingly appealing tool for many EU institutions, allowing them to cut costs and increase productivity. However, it raises many complex issues for data protection. It is for this reason that the topic has been addressed at our meetings with DPOs and in dedicated EDPS Guidelines.

In 2016, the European Commission launched the first inter-institutional Call for Tender for the provision of cloud-based IT services (Cloud I). As part of their cloud strategy, the Commission's Directorate General for Informatics (DG DIGIT) set up a subgroup within its Cloud Virtual Task Force (CVTF) to monitor the security and data protection controls offered by prospective contractors. The EDPS took part in the work of this subgroup, offering its expertise and advice where necessary.

Based on the outcome and lessons learned from Cloud I, DG DIGIT has put together a second Call for Tender for cloud-based products and services. We have followed the preparation of this Call for Tender closely and provided further advice to ensure that the obligations of the GDPR, for processors in particular, are taken into account at contractual and operational levels. Many challenges still remain to be addressed. We will therefore continue to invest efforts in this important issue, to ensure that the personal data of all EU employees and EU citizens is adequately protected.

@EU_EDPS

Need to find new ways for applying data protection principles to the latest technologies #bigdata #IoT #cloud computing #eudatap

Other IT initiatives within the EU institutions

The EDPS participates in several initiatives aimed at encouraging coordination and cooperation between the EU institutions on matters related to IT and IT security. These include the Inter-institutional Committee for IT (CII), for the IT managers of the EU institutions, the Information and Communication Technologies Advisory Committee of EU Agencies (ICTAC), the Security Subgroup of the CII and the Computer Emergency Response Team for EU bodies (CERT-EU).

This cooperation gives the EDPS direct access to the IT population of the EU administration. It means that we are both informed about relevant developments and trends relating to the IT infrastructure used by the EU institutions and that we are able to inform IT managers and practitioners working in the EU institutions about relevant developments in data protection.

With the support of the CII and ICTAC, for example, the EDPS was able to consult the IT community in the EU institutions during the preparation of Guidelines relating to IT matters, such as those on web services, mobile devices, mobile apps, cloud computing and IT governance and management (see Figure 14).

6.3 Facilitating responsible and informed policymaking

Almost all EU policy proposals now involve some form of personal data processing. In a world where policymakers must respond quickly to acute public security challenges and keep up with developments relating to the digital economy or international trade, the need for help to ensure that new EU proposals respect fundamental rights has never been greater.

The EDPS has consistently sought to provide support and guidance to the EU legislator. This has typically occurred in the form of formal

consultations on legislative proposals under Article 28 of Regulation 45/2001, or informal consultations based on a procedure agreed with the Commission back in 2009. As of December 2018, consultations are covered by Article 42 of Regulation 2018/1725, and the possibility for the EDPS to provide advice to other EU institutions and bodies, on request or on our own initiative, is laid down in Article 56 and 57 of the same Regulation.

Recognising the increasing number of EU policy initiatives now involving the processing of personal data, our Strategy set out several steps to improve the quality and efficiency of the guidance we provide to the legislator. These included identifying the areas in which help and advice were most needed and improving our collaboration with the European Commission, the Parliament and the Council.

6.3.1 Cybersecurity: ensuring privacy-friendly protection from cyber-attacks

A Eurobarometer survey published in September 2017 revealed that 87% of respondents considered cybercrime an important challenge to the internal security of the EU. The survey also showed that the most significant concern for internet users was the misuse of their personal data.

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. This Cybersecurity Package specifically mentioned the need to establish a system of EU cyber deterrence and criminal law that would better protect individuals, businesses and public institutions within the EU. The Commission elaborated on some of these initiatives in its report on the Security Union, published on 18 October 2017. We responded with Formal Comments on the proposed policy package on 15 December 2017, outlining our concerns and recommendations.

Adequate cybersecurity is necessary to protect privacy and personal data. However, prevention is also important. While we do need effective prosecution, it is even better to avoid becoming a victim of a cyber-attack in the first place.

With this in mind, we welcomed the Commission's commitment to avoid weakening or undermining the strength of encryption. Trustworthy encryption capabilities are critical for digital markets and societies. They protect data and help to inspire confidence in online services and cybersecurity tools.

In cases where the same tools can be used to protect personal data and for proactive cybersecurity, organisations will have to comply with both cybersecurity and data protection rules. It is essential that the Commission provide adequate guidance in the context of certification and incident management policies to avoid confusion or contradiction.

We stressed that any further measures to combat cyber criminals must be developed and applied with full respect for the data protection principles of necessity and proportionality. We also reminded the Commission that, as the EDPS has previously warned, if the tools we develop to counter cyber-attacks ever fall into the wrong hands they could be used against us. We therefore urged them to take this into account in any future work on the Cybersecurity Package (see section 6.4.4).

6.3.2 The single digital gateway: 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 in 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. It would help to improve the availability, quality and accessibility of information across the EU, by setting up a system in which individuals would only be required to submit certain documents once, and in one Member State only.

However, we recommended that the Commission take into account some important data protection considerations when developing the once-only principle further. These included providing additional clarity on some essential data protection principles, such as the legal basis of the processing of personal data, purpose limitation and data minimisation.

6.3.3 Digital content: the need for stronger consumer and data protection

The European Commission's proposal for a Directive on certain aspects concerning contracts for the supply of digital content aimed to extend consumer protection to digital content, whether this was supplied to a consumer in exchange for money or in exchange for data. In recognition of our efforts to improve cooperation between the EDPS and the Council, the Council requested an EDPS Opinion on the proposal.

On 14 March 2017, we published an Opinion, expressing support for the Commission's aim, which was to enhance consumer rights. However, we also highlighted the risk of confusion for consumers and businesses regarding 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 the consumption of goods and services, whether they are supplied in exchange for money or not.

At the same time, the GDPR legislates for the use of data in the digital economy, including the strict conditions under which the processing of personal data can take place in a contractual relationship. We therefore urged the EU to avoid creating legal uncertainty by inadvertently interfering with the rules provided by the GDPR and the future Regulation on ePrivacy (see section 6.1.5).

Though we recognise that developing the data-driven economy is essential for EU growth, ensuring trust in that economy depends on the protection of fundamental rights. The proposal on digital content, we argued, should be used as an opportunity to ensure that all future-oriented EU rules on data protection and consumer protection work together to further the interests of the individual.

6.3.4 mHealth: healthcare on the move

Mobile technology is revolutionising the healthcare market. All sorts of different options, catering to a wide range of health needs, are now available to the global population.

This convergence between technology and healthcare should provide individuals with access to better healthcare at a lower cost, improved control over their healthcare and easier and more immediate access to medical care and information online. However, it could also lead to the collection, purchase, sale and analysis of huge amounts of personal information, without the full knowledge and consent of the individual concerned.

On 21 May 2015, we published an Opinion on mobile health (mHealth), calling on industry, governments and consumers to address this issue. There is a need for transparency about how personal data is processed, shared and re-used and for what purposes. We warned that the failure to put data protection safeguards in place would result in a critical loss of individual trust. As a result, there would be fewer opportunities for public authorities and businesses, therefore hampering the development of the health market.

With the GDPR yet to be finalised at the time of publication, we stressed that future EU policies should encourage service providers and their associates to be more accountable for their actions. We called for an end to the indiscriminate collection of personal data and any possible discriminatory profiling and encouraged the implementation of privacy by design and by default in the development of mHealth technologies, as well as improved security measures. Respect for the choices of individuals should be at the core of all new technologies.

While individuals should be empowered to take a proactive approach to monitoring their health, this should not come at the expense of any loss of control over their personal lives in general.

Transparency, awareness and effective control over our personal information are integral to ensuring that this remains the case.

@EU_EDPS

Solutions on #mhealth should serve individuals, respect their choices and be ethically tenable and foster #trust #eudatap

6.3.5 Developing smart policies for smart technologies

Smart technologies are now ubiquitous in our digital society. Smart grids and intelligent transport systems are two examples of this.

Smart meters measure energy consumption and transmit this information to a chain of stakeholders tasked with the production, distribution and service provision of gas and electricity through smart grids. This process allows companies to offer more efficient energy production and distribution, with cost savings for both the service provider and the customer.

Through the WP29, the EDPS has been involved in a project launched by the European Commission designed to ensure the security and protection of personal data in this process since 2012. This included providing advice on the Commission's Smart Grid Data Protection Impact Assessment template.

In January 2016, some major European utility companies presented their experiences working with this template at a workshop held at the Commission's Directorate General for Energy (DG ENER). As Assistant Supervisor Wojciech Wiewiórowski highlighted at the workshop, this was a hugely valuable exercise in advance of the GDPR, which makes DPIAs obligatory in cases where the processing of personal data is considered high risk for individuals. The European Commission presented the final version of the template to the public in October 2018, taking into account the final provisions of the GDPR and available guidance from the EDPB.

Cooperative intelligent transport systems (C ITS) are a group of technologies and applications that allow vehicles to connect with one another and with other elements of the transport system, such as traffic control or toll collection systems. They aim to help avoid collisions and contribute to road safety, as well as to improve the flow of traffic.

Privacy considerations are very important in the deployment of C ITS, as the technology used can collect huge amounts of data which could be used for profiling or tracking people.

In November 2014, the European Commission launched its C ITS platform. As part of the data protection sub-group on this initiative, we have followed developments closely over the course of the mandate. In particular, we have focused on drawing attention to any possible challenges relating to the preservation of data quality and security and to facilitating accountability and purpose limitation. We also highlighted the need to ensure transparency and the protection of personal data, and recommended that particular attention be given to facilitating privacy by design, defining roles and responsibilities, identifying security concerns and informing users about the collection, storage and usage of their personal data.

6.4 Promoting a mature conversation on security and privacy

Public security, combatting crime and fighting terrorism have always been important policy concerns for the EU. Over the course of the mandate, the urgent need to address these issues has only increased, largely due to several high profile and tragic events. However, while threats to individual and societal security are very real, we need to ensure that our responses are both necessary and proportionate. Any response that interferes excessively with our fundamental rights will only reduce public trust in governments, undermining any efforts to address common security concerns.

We strongly believe that increased security can be achieved without unduly restricting

data protection rights. This is why we made a commitment to promoting a mature conversation on security and privacy. This conversation focuses on finding innovative legal and technological solutions that strike the correct balance between the protection of fundamental rights and the need for increased security measures. It is important to stress, in this context, that Article 6 of the Charter, covering the right to liberty and security, is intended to protect individual liberty and security against the State, not to guarantee it through the State.

This is an ongoing area of discussion. With threats to EU security unlikely to diminish any time soon, it is vital to ensure that this conversation continues at the highest levels. The EDPS will therefore continue engaging directly with the EU institutions and bodies working in these areas and providing policymakers with the tools they need to help them develop adequate solutions.

6.4.1 Privacy-friendly policymaking made easier

To comply with EU data protection rules, any measure proposed by the EU legislator that involves restricting data protection rights must be both necessary and proportional. This is a particular concern for policies relating to EU security. However, assessing the necessity and proportionality of proposed measures, especially when working under pressure, is not an easy task for EU policymakers. For this reason, the EDPS developed a Necessity Toolkit and Proportionality Guidelines.

Using an evidence-based approach, policymakers must be able to demonstrate that any planned limitation of the fundamental rights to data protection and privacy 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.

To assist policymakers in doing this, we published a Necessity Toolkit on 11 April 2017. The Toolkit 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.

Just as policymakers should be able to demonstrate that any measure that would limit fundamental rights is absolutely necessary, they also need to be able to demonstrate that the measures proposed are proportional, taking into account the policy aims and purpose of the data processing proposed. To help them with this, we developed Guidelines for policymakers on how to assess proportionality. These were submitted to an open consultation on 25 February 2019.

The Guidelines propose a test consisting of four criteria against which policymakers can evaluate the proportionality of any new measure, and thus adjust their proposal accordingly. They also include examples, which aim to demonstrate how any unjustifiable limitation to the right to data protection can have a negative impact on other fundamental rights and freedoms. This shows that measures affecting privacy and data protection not only have repercussions for the individuals directly concerned, but also for society as a whole.

As for the Necessity Toolkit, the Guidelines on Proportionality take into account existing guidance from the Commission and the Council on how to verify the compatibility of new EU laws with the EU Charter. Both also refer to existing European case law and recent EDPS legislative Opinions and formal Comments.

As almost all EU policy proposals now involve some kind of personal data processing, it is vitally important to ensure that policymakers are well-

@EU_EDPS

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

equipped to adequately assess the necessity and proportionality of a proposed measure. The EDPS Guidelines on Proportionality and the Necessity Toolkit encourage policymakers to consider these key dimensions from the start of the legislative process, therefore facilitating responsible and informed EU policymaking.

6.4.2 Debating the future of information sharing in the EU: interoperability of large-scale IT systems

In order to address challenges relating to security and border management, the EU must adopt a smarter approach to information sharing. One tool that could prove useful in this respect is interoperability. However, interoperability is also likely to have profound legal and societal consequences, which must be carefully assessed and addressed before putting interoperability into practice.

As outlined in our reflection paper on the topic in November 2017, although the interoperability of information systems is often thought of as a merely technical concept, it cannot be disconnected from questions about whether it is necessary, politically desirable or legally possible.

On 16 April 2018, we followed up our reflection paper with an Opinion on the proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems in the fields of migration, asylum, border management and police and judicial cooperation. Interoperability would allow these large-scale EU databases to communicate and exchange information.

The proposals provide for the possibility to use the systems more extensively, beyond the specific objectives for which they were originally set up. In particular, the data stored in the different systems would be gathered in order to combat identity fraud, but also to facilitate and allow for identity checks within the Member States' territories. They would also facilitate law enforcement access to databases that do not contain law enforcement information.

Particularly concerning for the EDPS was the proposed creation of an EU centralised database containing information about millions of non-EU citizens, including biometric data. If a data breach were to occur, the scale of the database and the nature of the data to be stored within it could cause significant harm to a very large number of people. To assess whether such a database is necessary, the extent of the problem of identity fraud among non EU-citizens needs to be clearly demonstrated. The purpose of the identity checks within Member State territory also needs to be precisely defined, as the identification of a person is not an end in itself but needs to serve a specific objective.

Law enforcement authorities need access to the best possible tools to fight terrorism and other serious crime. However, facilitating law enforcement authorities' access to information not originally collected for law enforcement purposes has significant implications for the protection of fundamental rights. Strict and appropriate legal, technical and organisational safeguards must therefore be built in to all EU databases, and particular attention must be given to defining the purpose of such access and the conditions under which the information can be used.

Taking into account the implications of interoperability for fundamental rights, we called for a wider debate on the future of EU information exchange, the governance of EU information systems and on how to safeguard fundamental rights in this context. To facilitate this debate, in 2019, the EDPS organised a panel on this topic at the Computers, Privacy and Data Protection Conference (CPDP). The aim of the panel was to debate the EU response to the migration crisis and the security challenge that relies to an important extent on the interoperability of EU large scale IT systems. We also organised a workshop on interoperable Information Systems in the EU Area of Freedom, Security and Justice together with the European University Institute's (EUI) Department of Law and Migration Policy Centre (MPC) and the Centre for European Policy Studies (CEPS).

6.4.3 Supervising europol

A secure and open Europe requires improved operational effectiveness in the fight against serious crime and terrorism, but it also requires a commitment to protecting the fundamental rights and freedoms of individuals.

@EU_EDPS

New Regulation boosts the roles of #EDPS and @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. It is the job of the EDPS to ensure that it does so in compliance with data protection rules (see chapter 1).

The EDPS and europol

As one of Europol's supervisory authorities, the EDPS is the guardian of fundamental rights and freedoms in the field of law enforcement. We therefore engage in a constructive dialogue with Europol to protect privacy when dealing with data processing for the purpose of law enforcement.

The results of this dialogue often have an impact across the wider law enforcement community. The very nature of Europol as an Agency means that it performs its tasks in constant interaction with the competent authorities of the Members States, as well as with its partners across the globe. This means that any data protection regime implemented at Europol has a wider effect than simply what happens inside Europol headquarters. Not only is the data exchanged with Europol partners appropriately protected by its strong data protection regime, but the data protection framework put in place by Europol may also inspire partners to assess and enhance their own standards. Another way Europol continually exports its data protection expertise is through the numerous meetings and conferences it hosts, and in which the EDPS participates as much as possible.

We are very much aware of the wider context in which Europol operates and we aim to take this into account in our work with them. Our cooperation with other DPAs through the Europol Cooperation Board helps ensure a common approach throughout Europe with regard to data protection (see section 5.3.1).

The supervision of data processing activities in the field of law enforcement involves a number of challenges. First, this is a domain where individuals' rights are restricted, justifying derogatory regimes. In addition, the impact of such data processing activities on individuals' rights and freedoms is high. Personal data is collected and processed in order to allow public authorities to take decisions, which can have a serious impact on individuals' rights, even more so as many of the individuals concerned belong to vulnerable groups of people. Finally, such data processing activities are opaque to individuals. It is difficult for data subjects to know who is processing their data and for what purposes. As far as Europol is concerned, the supervision of these data processing activities is made more difficult by the fact that Europol IT systems are complex and process a large volume of personal data. Europol is active in many crime areas, which all have different imperatives and constraints.

The EDPS therefore has a specific role: ensuring that individuals' rights are effectively protected, as individuals do not have the power to exercise this control to the same extent as in other areas.

Preparing for our new role

Throughout 2015 we provided advice to the legislators on specific data protection issues related to the Europol Regulation. In December 2015, the legislators agreed on a final text. The new Regulation designated the EDPS as supervisor for the processing of personal data relating to Europol's operational activities, taking over the majority of the tasks previously performed by the Joint Supervisory Body of Europol (JSB). The Regulation was approved on 11 May 2016 and has been in place since 1 May 2017.

Preparations for our new role involved setting up a dedicated internal taskforce involving all EDPS units and sectors. EDPS staff members followed internal and external training courses related to Europol supervision and we established regular contact with the Data Protection Function team (DPF) at Europol, to foster mutual understanding and establish effective communication channels. High-level meetings also took place between EDPS Giovanni Buttarelli and Europol's then-Director Rob Wainwright in 2016.

On 15 and 16 May 2017, just after taking over our new responsibilities, we organised an operational visit to Europol, which helped us to familiarise ourselves with Europol's practices and procedures.

To ensure we were aware of the current issues at stake in Europol supervision and to prepare cooperation with Member States, 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.

Since taking on our new role at Europol on 1 May 2017, we have put in place a structured system of supervision designed to encourage cooperation and ensure accountability.

Cooperation with europol

We work closely with Europol's DPF team and other operational staff, providing them with informal advice when required, notably through bi-monthly meetings. This helps us to anticipate consultations and other issues on data processing and to define and plan for future activities, such as inspections or inquiries.

Cooperation at management level is equally important and meetings between the EDPS and Europol higher management take place periodically.

Cooperation with other supervisory authorities

As most data processed by Europol originates from Member States, Europol's supervision also requires close cooperation with the relevant supervisory authorities in the Member States. While it is our responsibility to supervise the processing of personal data by Europol, each national DPA is responsible for overseeing 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.

For this reason, the Europol Regulation provides for the establishment of a Cooperation Board, made up of representatives from national DPAs and the EDPS. The Board works as an advisory body on matters involving the processing of personal data by Europol which originate in the Member States. The EDPS provides the secretariat for this Board, which meets at least twice a year (see section 5.3.1).

Much of the cooperation occurs through the Cooperation Board, but we also cooperate with representatives from the DPAs to carry out inspections.

The EDPS reports to the Joint Parliamentary Scrutiny Group (JPSG), which monitors Europol, at least once a year, to discuss Europol's compliance with the rules and principles relating to the protection of personal data.

Supervisory activities

To ensure effective supervision, the EDPS actively monitors actual compliance with data protection rules, either on our own initiative or following a complaint.

The Europol Regulation allows for the processing of personal data for operational analysis, to support criminal investigations and criminal intelligence operations carried out by law enforcement authorities in the Member States. However, they can only do so as part of operational analysis projects (OAP). Europol is required to inform the EDPS about the purpose, the categories of data and the individuals involved in each OAP, as well as the participants, data retention period, conditions for access and any proposed transfer or use of the data concerned.

We provide advice on all matters concerning the processing of personal data at Europol, in the form of Opinions. Moreover, whenever Europol plans a new data processing activity involving the processing of sensitive data or the possibility of significant risk to an individual, they must notify the EDPS providing a general description of the envisaged processing operations, an assessment of the risks to the freedoms of individuals and the measures envisaged to

Figure 15. Europol Prior Consultations

address those risks. We examine their proposals and provide recommendations (see Figure 15). So far, we have received six prior consultations and issued an equal number of opinions.

We also carry out general and thematic inspections at Europol. These inspections are the cornerstone of our supervisory activities, and we have completed three inspections since May 2017. The first took place in December 2017 and subsequent inspections followed in May 2018 and June 2019. In each one of them, we carefully audited selected legal and technical aspects of data processing. Our inspections also include a check on the compliance of data security following international standards. During these inspections, we took into account critical open recommendations from the last inspection of the JSB. Notably, we checked the processing of personal data in OAPs, the data breach procedure and the Europol Information System (EIS).

We invite experts from national DPAs to join our general inspections. The Member States are Europol's main information providers so the participation of national experts in the inspection process helps to raise awareness of any problems arising at Europol level that might have originated at national level. This could include problems with data quality or insufficient justification for the processing of sensitive data or data on special categories of persons such as minors. Back home, national experts can consider how to tackle these problems in their own supervisory activities. This helps increase the coordination between EU and national supervisory activities.

On 5-6 February 2019, we also carried out a targeted inspection on the verification role assumed by Europol in the implementation of the Terrorist Financing Tracking Programme (TFTP) Agreement between the EU and the US.

Following our on-site activities, we outline a number of recommendations for improvement in an inspection report that is sent to the Executive Director of Europol and shared with the Cooperation Board. We closely follow up on these to ensure that Europol put EDPS recommendations into practice. Our findings

provide the opportunity to initiate activities aimed at improving the level of data protection and the efficiency of Europol's operational activities.

Apart from inspections, we conduct own initiative inquiries on issues that come to our attention in the course of our other supervisory activities. We also deal with any complaints from individuals relating to the processing of their personal data by Europol.

Europol has the obligation to inform us of any personal data breach that might occur without undue delay. In such cases, Europol also has the obligation to assess the negative impact of the data breach on the rights and freedoms of the individuals concerned and inform them in case this is significant. From the beginning, we have monitored Europol's internal procedure for dealing with such cases through our bi-monthly meetings and provided our input.

Communication

Building on the expertise acquired throughout the supervision of Europol, the EDPS contributes to the public debate on security and privacy in the law enforcement community.

For example, on 22 November 2018, Assistant Supervisor Wojciech Wiewiórowski gave the keynote speech at a conference on Freedom and Security, jointly organised by the Europol Data Protection Experts Network (EDEN) and the Academy of European Law (ERA). Several EDPS staff members also regularly take part in conferences and events dealing with data protection and policing, both as participants and as speakers.

Looking to the future

After two years of supervising Europol, we have established strong links with Europol and have developed a good knowledge of the issues they face when implementing data protection in practice. New challenges will require specific scrutiny from the EDPS. This includes the emergence of structural data exchanges between justice and home affairs agencies in the EU institutions, between national authorities and EU agencies and the use of new technologies, such as Big Data or Artificial Intelligence.

6.4.4 Intrusive surveillance technologies

On 15 December 2015 we issued an Opinion on intrusive surveillance technologies.

In July 2015, the internal emails, sales details and technical documentation of a company selling surveillance tools to government customers, inside and outside the EU, were leaked to the public. The documents also described in detail the capabilities of these tools, which were being used by governments and law enforcement authorities to investigate the lives of individuals.

Our Opinion aimed to draw attention to the risks posed by the unregulated and growing market for the sale, distribution and use of such tools. We emphasised that more needs to be done to monitor the market and called on legislators to look for safeguards that embed privacy by design in technology and ensure that it is secure.

Governments claim that there exists a need for the legitimate and regulated use of surveillance tools by law enforcement bodies. However, it must be recognised that they can also be used to circumvent security measures in electronic communications and data processing, thereby undermining the integrity of databases, systems and networks.

As our digital lives become increasingly connected, the risks will only increase. A coordinated approach to tackle these risks, including better regulation of the trade and use of surveillance software, is therefore necessary in order to ensure the privacy of all individuals in the EU is adequately protected, both at home and abroad. The GDPR goes some way towards addressing this, by specifically including the principle of data protection by design, for example, which in this case would mean ensuring that tools for use in law enforcement activities do not have technical capabilities beyond those allowed for by law. More, however, still needs to be done.

7. COMMUNICATION AND RESOURCE MANAGEMENT

7.1 Information and communication

A new mandate meant a new approach to communication activities at the EDPS. This involved a new image, as well as new communications tools and a general revamp of our communication strategy. Establishing ourselves as a global leader means ensuring that the important work done at the EDPS reaches its intended audience.

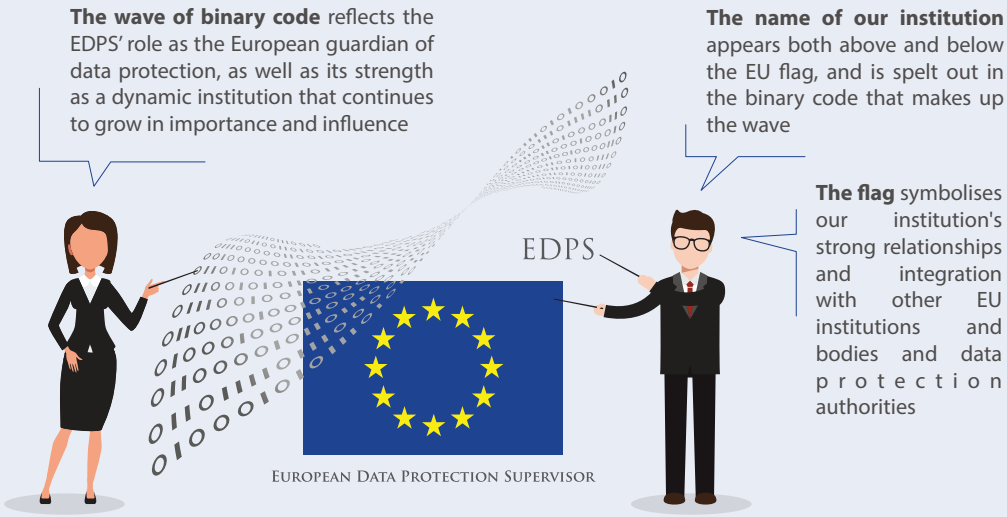
Data protection needs to be understandable and accessible. Everyone needs to be able to understand their rights and obligations, yet we are fully aware that many people perceive data protection as technical and obscure. There are too many important issues at stake for us to risk our messages not being heard. Our focus has therefore been on communicating in a clear, concise and transparent manner across all of our communication channels.

Establishing a new visual identity, launching new initiatives and improving the way we use existing channels of communication have all been integral to establishing the EDPS as a leading global voice on data protection and privacy issues, whether we are speaking to data protection experts or the average EU citizen.

7.1.1 A new visual identity

In May 2015 we launched a new EDPS logo. This was part of a process to develop a new visual identity for the institution, reflecting a new era

THE EDPS LOGO



in the history of the EDPS as a global leader on data protection and privacy issues. It was the first stage in a rebranding project spanning the first half of the mandate.

With the logo finalised, we focused our attention on rebranding our website. We wanted to make it more user-friendly, ensuring that it was easier to navigate and more transparent.

We completed the first stage of this rebranding process in November 2015, when we launched a new-look website, incorporating a variety of new features designed to increase accessibility and transparency. These included:

- an agenda;
- a responsive design for use on smartphones and tablets;
- a new layout for the homepage.

Work on the website continued throughout 2016, with the aim of going live with a brand new EDPS website in early 2017. This involved designing a new layout for the website, migrating content from the old website to the new one and transitioning to a new content management system (CMS), EC Drupal.

In March 2017 we launched the new EDPS website. The new layout provides easy access to EDPS work, which is organised by topics, and to social media, through a Twitter wall. We added new content, such as the history of the GDPR and our latest blogposts and videos, to the homepage and incorporated a powerful new search engine, making it easier for users to find the information they need.

We have made various improvements and changes to the website since 2017, in an attempt to address issues raised by both EDPS staff members and external users. This includes introducing a Quick Links section to the homepage, to provide users with a shortcut to some of the most frequently used pages on our website. Where possible, we also moved from publishing documents in PDF format to producing them in HTML, ensuring an improved user experience on mobile phones and tablets.

In order to ensure that our website remains as data protection friendly as possible, in early 2019 we also moved from opt-out tracking to an opt-in process. This means that we are only able to track visitors to our website if they explicitly provide us with consent to do so.

Next up for a revamp was the EDPS Newsletter. With the number of subscribers to our Newsletter growing year on year, the Newsletter is a valuable tool for communicating about our most recent and important activities. By switching to a new, online, mobile-friendly format, we intended to make the Newsletter more accessible and user-friendly, regardless of the device used to read it.

We distribute Newsletter to our Newsletter mailing list and publish it on our website. Though the content largely 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 issued in June 2017, with ten editions now published every year. A survey of Newsletter subscribers carried out in May 2019 revealed that our readership are generally satisfied with the Newsletter in its current form.

@EU_EDPS

EDPS' new logo - new era in the history of our organisation

7.1.2 New initiatives

In July 2015 we released a mobile app. This allowed users to compare EDPS recommendations on the GDPR against the texts produced by the European Commission, Parliament and Council. The app was updated in 2016 to allow users to view the final text of the GDPR alongside the Commission's initial legislative proposal, the recommendations provided by the EDPS and the rules outlined in the previous Data Protection Directive 95/46/EC. The app also provides a history of the reform process (see section 6.1.1).

The app was an innovative way for the EDPS to encourage the legislator to implement

pragmatic solutions, by holding them to account, and to contribute to the transparency and accountability of the legislative process.

Another new initiative, launched in April 2016, was the EDPS blog. The blog provides a more detailed insight into the work of the EDPS, and of the Supervisors in particular. It allows the Supervisors to communicate on a more personal level about their thoughts, opinions and activities, as well as the work of the institution. We wanted to make our work, and data protection in general, more accessible and understandable and, in doing so, try to reach new audiences.

The EDPS blog is now an integral part of our communication activities. We publish new blogposts on a regular basis and on a wide range of topics, including current policy concerns and independent initiatives launched by the EDPS. All blogposts are promoted through our social media channels and some of our blogposts are distributed to our network of journalists and other interested parties. All blogposts can be easily found from the homepage of our website.

7.1.3 Social media

Social media has become indispensable as a communications tool for the EDPS. Over the course of the mandate we have firmly established our presence on three influential social media channels, through which we are able to quickly and easily reach a global audience.

While Twitter remains our most influential social media tool, our presence on LinkedIn has witnessed the most dramatic growth over the past five years, going from just 877 followers at the end of 2015 to 16,344 by 30 September 2019. Engagement through our YouTube channel has also increased, largely as a result of our communication efforts during the 2018 International Conference of Data Protection and Privacy Commissioners.

Our continued growth on social media is testament both to our increasing global influence as an organisation and our efforts to implement an effective social media strategy.

7.1.4 The GDPR for EUI: the communication campaign

The new data protection rules for the EU institutions became fully applicable on 11 December 2018. To complement our awareness-raising efforts (see section 6.2.1), we launched a communication campaign. Though aimed principally at EU institution staff members, we also wanted to raise awareness among those outside the EU institutions about how the new rules might affect them and their rights.

We put together a Communications kit, including relevant and helpful information for all EU staff members. This was distributed to all EU institution data protection officers (DPOs) in advance of 11 December 2018 and was designed to help them to reach out to staff members working in their respective institutions.

The kit included a video on accountability, a poster for DPOs to print and distribute in their buildings, artwork for use on their intranet or social media channels and webcam covers to be distributed among some EU staff members. We also created three new factsheets, on data protection rights under the new rules, the implications of the new rules for EU employees and on ensuring accountability, copies of which were available in the kit and on our website.

In addition, individual copies of the new Regulation were prepared and distributed among DPOs at the EDPS-DPO meeting, which took place on 12 December 2018 (see section 6.2.2).

To complement our cooperation with DPOs, we also launched a press and social media campaign, aimed at raising awareness outside the EU institutions. We used Twitter and LinkedIn to provide information about the new rules, their implications and the role and activities of the EDPS. We also published a press release and contacted some media outlets directly to try to ensure coverage. An advertisement, featuring an engaging cartoon, was published in Politico on 13 December 2018 to support the campaign, while we also made efforts to bring our website and Wikipedia entry up-to-date, to reflect the changed legislation.

7.1.5 Preparations for the EDPB - communication

As a new EU body, the European Data Protection Board (EDPB) required its own visual identity (see section 6.1.3). In 2017, we presented several designs for an EDPB logo to members of the Article 29 Working Party (WP29), from which one was selected. We then developed a corporate identity around this logo, specifying how it could be used.

The new body also required a website and the transition to a new EDPS website served as the starting point for its creation. Moving the EDPS website to a new CMS, EC Drupal (see section 7.1.1), was a strategic move, providing us with greater flexibility, both in how we present our work on our own website, but also in the creation of additional websites, including the EDPB website. We started work on the EDPB website in 2017, completing it in time to launch the website on 25 May 2018, the day that the GDPR became fully applicable.

Though the EDPB secretariat has its own communications team, we have continued to provide support as and when required, whether with publications, videos or the organisation of events. We work closely with all members of the EDPB through the EDPB Communications Network, in an effort to better coordinate the communication efforts of the data protection authorities (DPAs) across the EU and support each other in our work.

7.1.6 The 2018 international conference - communication

Communication on the 2018 International Conference, co-hosted in Brussels by the EDPS (see section 5.2.1), kicked-off at the 2017 edition of the conference, which took place in Hong Kong. We had the chance to promote the 2018 conference through a video, in which we introduced the topic and the questions we aimed to explore. We also distributed an information leaflet about the conference.

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

Work on the conference website also began in 2017. As with the EDPB website, we were able to use the move to EC Drupal to our advantage in creating the conference website. We launched the website on 19 March 2018. It provided all relevant information about the conference theme, programme, speakers and venues, and also served as the portal for conference registration. Participants in the closed session were also able to access all meeting documents through the website, using their login details and password. We kept the website up to date throughout the conference by promptly uploading documents, videos and news as soon as they were available to us.

To encourage participants to get involved in the wider online debate, in 2017 we set up a Twitter account for the event. We then reinforced our social media efforts in 2018, with the introduction of an Instagram account. We were active on both of these channels throughout the conference, providing regular updates, information and coverage of the conference. We supported our efforts using the EDPS social media accounts.

In 2017 we also started work on the creation of a mobile app, to be used to encourage audience participation in the conference. This was available to download a few weeks before the conference and all delegates were encouraged to download it for use during the public session. It reflected and complemented the conference website. Participants were able to use it to take notes, take part in polls, share their views and send questions to the conference host for speakers to answer on stage.

All of these efforts were accompanied by a media campaign, directed at the international media. This included a press conference and press release on the first day of the public session. The overwhelming press coverage we received from all over the world reflected global interest in both the topic of discussion and the speakers involved in the conference.

7.2 Administration, budget and staff

The EDPS Human Resources, Budget and Administration (HRBA) Unit provides support to the Management Board and operational teams at the EDPS, ensuring that they have the tools and resources to achieve the goals set out in the EDPS Strategy 2015-2019.

This work has involved recruiting, managing, developing and reinforcing our staff in order to broaden our expertise and capabilities, as well as ensuring that the EDPS leads the way in data protection accountability, setting an example for others to follow.

In addition to this, we have been involved in two significant EDPS projects over the course of the mandate: the establishment of the EDPB secretariat and preparations for the 2018 International Conference of Data Protection and Privacy Commissioners.

7.2.1 A growing organisation

The EDPS grew significantly between 2015 and 2019. One of the main reasons for this was a need to hire more data protection experts, to help us ensure that we were able to take on a range of new roles and perform them competently and effectively. This included providing the EDPB secretariat, taking on responsibility for Europol supervision and ensuring that we had the personnel and expertise to carry out the tasks assigned to us under the new Regulation 2018/1725. We also needed to be able to cover usual staff turnover.

In addition to this, data protection scandals, new technologies and the new EU data protection framework have led to greater public consciousness about data protection rights and obligations. There is now a greater demand for the services of DPAs, the EDPS included, than ever before. We need to ensure that we are able to respond, in order to ensure the protection of individuals' rights.

To accommodate the need to reinforce our staff, in late 2014 we asked the European Personnel Selection Office (EPSO) to organise a competition for data protection specialists. A reserve list was established, from which we were able to recruit new staff members, starting in 2015.

Having exhausted this reserve list by 2018, we launched a new open competition for 30 Administrators in the field of data protection in summer 2018. This list was finalised in mid-2019, providing us with a new pool of experts from which to recruit staff members. This will help us to cope with the growth of the EDPB secretariat and to perform new tasks assigned to us by the legislator, such as the supervision of Eurojust and the European Public Prosecutor's Office. The EDPS has been preparing to take on the supervision of Eurojust, starting on 12 December 2019, since the end of 2018, through regular contact with our Eurojust counterparts, the exchange of knowledge, awareness raising and the identification of priorities for the first months of supervision.

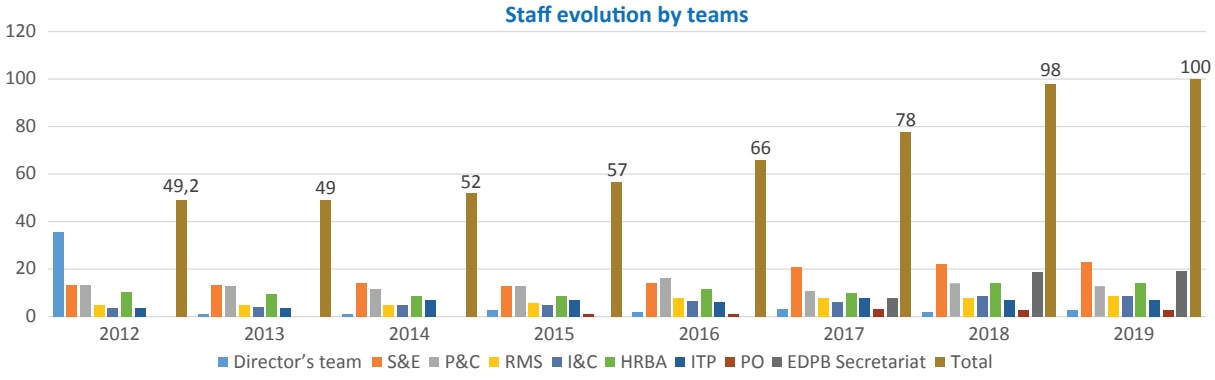


Figure 16. Staff evolution by teams (up to 30 June 2019)

In addition to organising these competitions, we also adopted a staff retention policy in 2016, which we reviewed again in 2017, taking into account the results of our 2016 staff survey. The policy focused on making sure that we are able to retain the talented, knowledgeable and creative staff members we recruit, by offering more flexible working conditions and increased opportunities for personal and professional development, as well as encouraging and reminding managers to keep their staff motivated by providing recognition and constructive feedback.

With a new recruitment plan in place, we faced the challenge of accommodating our growing staff population. We launched an ongoing project focused on maximising the office space already available to us as well as acquiring new space. To house the EDPB secretariat, we took over the first floor of our current building, creating a clear separation between the secretariat and the EDPS. A programme of office reorganisation and renovations was also launched to accommodate new EDPS employees. Further progress in this area is expected over the coming months, as we endeavour to find a solution to accommodate our expanding institution.

7.2.2 Learning and development

In July 2015, we adopted a new strategy on learning and development (L&D) at the EDPS, aimed at fostering staff development and broadening expertise. Under the new strategy, every year each EDPS staff member develops their own L&D plan, allowing us to adopt a longer-term perspective on the learning and development needs of our staff.

We also began a programme of tailor-made training sessions, conducted in-house and customised to the specific needs of EDPS staff members. Over the course of the mandate topics for these training sessions have included public speaking and media training, Key Performance Indicators (KPIs) and impact assessment, tools and procedures used by the EDPS and the EDPB, the new data protection rules for EU institutions and the General Data Protection Regulation (GDPR) and raising awareness of unconscious biases, burnout and other issues.

To complement this, in 2017 we launched a major project aimed at providing career guidance to all EDPS staff. This exercise helped us to identify staff members interested in working for the EDPB secretariat, but it was also a chance to help EDPS employees to think about their career progression. Individual, confidential career guidance sessions were provided to all staff members except for managers, and took place on a voluntary basis. Follow-up sessions and actions were organised where helpful.

In 2019, we launched the internal coaching initiative. The purpose of this coaching is to improve individual job performance by managing performance and talent, resilience and development as well as relationships at work. It focuses on developing strengths and making sought-after changes, as well helping to find specific solutions to professional challenges. Sessions take place with our internal coach.

7.2.3 Setting up the EDPB secretariat - administrative preparations

Providing an independent secretariat to the EDPB (see section 6.1.3) was a logistical and organisational challenge. This was because we had to ensure confidentiality and the separation of functions while simultaneously preserving administrative cooperation and value for money.

Administrative preparations for the future EDPB began as early as 2013, in cooperation with our colleagues in the WP29. In late 2015, once the European Parliament and the Council had reached a political agreement on the text of the GDPR, we ramped up our efforts, establishing a small internal EDPS taskforce and contributing to a separate taskforce set up within the WP29. Our goal at this stage was to assess the task facing us and determine exactly what was required in order to ensure that the Board could be operational from day one.

As the authority responsible for providing the EDPB secretariat, we had to ensure that the EDPB received adequate human and financial resources from the budgetary authority and that the necessary administrative set-up was in place. In 2016, we therefore implemented an ambitious recruitment plan, including the

resources needed to staff the future EDPB. We also produced four information factsheets on the setting up of the EDPB, outlining our vision. These covered early preparations, human resources, budgetary and financial resources and Service Level Agreements signed by the EDPS. Our aim was to help members of the WP29 to better understand our vision and the energy we were investing in setting up the EDPB.

With preparations for the EDPB in mind, the EDPS was also involved with the development of the European Commission's AGM project, aimed at improving the organisation of meetings and the exchange of meeting documents. In September 2016, we were designated as one of the pilot organisations for this project.

AGM is an IT application designed to aid in the management of expert groups and committees, and is therefore a tool of significant benefit to the EDPS and the EDPB secretariat, allowing us to automatically process a number of time-consuming tasks that would otherwise require the work of several staff members.

We have been using the system since December 2016 for the organisation of EDPS meetings, EDPB plenary meetings, subgroup meetings and other ad-hoc meetings. This provides us with an electronic workflow for the invitation and reimbursement processes of government experts. Statistics on the number of reimbursement files per year until 30 June 2019 can be found in Figure 17.

In November 2017, we established a sector in charge of EDPB matters. Several EDPS staff members were transferred to this new sector, charged with carrying out the tasks necessary to ensure that the EDPB would be ready to start work in May 2018. In March 2018, these staff members were moved into offices on the first floor of the EDPS building.

We needed to ensure that all staff members transferred from the EDPS to the EDPB, as well as any new EDPB staff members, would benefit from the same rights and be subject to the same rules as those working for the EDPS. We therefore carried out a review of all existing decisions, guidelines and manuals and a general decision was signed by the EDPS Director. While some specific decisions still needed to be updated after 25 May 2018, to take into account some peculiarities relating to the EDPB secretariat, the majority of the work was completed on time.

We also had to update our service-level agreements (SLAs) with external providers. While those covering EDPS staff members were automatically applicable to staff members of the EDPB secretariat, those relating to the provision of services needed to be updated to ensure that EDPB staff members could make use of those services. At the beginning of 2018 we therefore updated several SLAs to include the EDPB. In other cases, new SLAs were signed directly between the EDPB secretariat and the service provider. In this way, we were able to ensure business continuity and a smooth start for the EDPB secretariat.

With the EDPB up and running, we launched a pilot secondment programme in 2019. The GDPR entrusts the EDPB, and others, with the task of promoting the exchange of information, practices and common training programmes and facilitates the exchange of personnel between supervisory authorities. The EDPS HRBA unit has significant experience in the organisation of similar exchanges, and so we proposed to facilitate a process involving the exchange of staff members between DPAs or with the EDPB secretariat. The draft programme was discussed at a meeting between HR and L&D representatives from the DPAs in September 2018, and the first edition of the programme is due to take place in 2020.

AGM transactions up to 30/06/2019					
	2016	**2017**	**2018**	**2019**	**Grand Total**
Number of trasactions	16	83	733	776	1608

Figure 17. Number of AGM transactions (up to 30 June 2019)

@EU_EDPS

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

7.2.4 The 2018 international conference - finance and procurement

In addition to choosing a non-traditional theme for the 2018 International Conference (see section 5.2.1), the EDPS relied on a more unconventional way of financing the conference. As an independent supervisory authority, we took the decision not to use sponsorship to deliver the closed and public sessions of the conference in Brussels, relying instead on the conference registration fees to finance them.

The EDPS is an EU institution and therefore has to comply with the strict procurement procedures set out in the EU Financial Regulation. As the organisation of the conference involved the time-consuming and complex task of identifying, selecting and contracting external providers, we decided to hire the services of a company specialised in event organisation to help and support the EDPS finance team. We developed a specific financial procedure for the Conference, facilitating operations between the EDPS, the event organiser and external providers.

To support staff members and the Supervisors in their preparations for the conference, we also organised a number of communication training courses throughout 2018.

7.2.5 Preparing the EDPS for new data protection rules

As an EU institution, the EDPS is not only responsible for supervising and enforcing the new data protection rules within the other EU institutions and bodies, we also need to apply them to our own work and try to set an example for other institutions to follow.

As Regulation 2018/1725 affects numerous HR and Finance decisions, we launched a full review of our HR data processing activities. From early 2017, we participated in the internal Task Force on the Project Transition to new Regulation 45 and worked closely with the EDPS DPO, Assistant DPO and Supervision and Enforcement Unit to draft data protection records. We also revised our data protection notices. This allowed us to be fully prepared when the new Regulation entered into force.

We were also closely involved in internal discussions on the creation of an EDPS accountability tool. In 2015, the EDPS launched a project to develop a framework for greater accountability in data processing, which we applied to the EDPS as a test case, over the course of 2016.

The tool consisted of a set of questions for the Supervisor, Director, DPO and staff members responsible for managing processing operations, aimed at ensuring that the institution is in control of personal information and its lawful processing. The HRBA Unit provided feedback to the EDPS DPO on the questions relating to our area of activity. Once the tool was finalised in May 2016, the accountability officer at the EDPS set up a roadmap for answering the questions, providing evidence and creating an internal action plan for the HRBA Unit.

We continued to use the tool throughout 2017, also updating the questionnaire. It has helped us to demonstrate the accountability of the Unit, in particular our readiness to ensure compliance with data protection obligations and to produce documentation to prove this.

ANNEX A - LEGAL FRAMEWORK

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

Since the entry into force of the Lisbon Treaty on 1 December 2009, Article 16 TFEU provides the legal basis for the EDPS. Article 16 underlines the importance of the protection of personal data in a more general way. Both Article 16 TFEU and Article 8 of the EU Charter of Fundamental Rights establish that compliance with data protection rules should be subject to control by an independent authority. At the EU level, this authority is the EDPS.

Other relevant EU acts on data protection are:

- Directive 95/46/EC, which was replaced by Regulation 2016/679, the General Data Protection Regulation (GDPR), on 25 May 2018. The GDPR lays down a general framework for data protection law in the Member States
- Directive 2002/58/EC on privacy and electronic communications (as amended by Directive 2009/136). A new Regulation on privacy and electronic communications (ePrivacy) is currently under negotiation
- Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Background

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms provides for a right to respect for private and family life, subject to restrictions allowed only under certain conditions. However, in 1981 it was considered necessary to adopt a separate convention on data protection, in order to develop a positive and structural approach to the protection of fundamental rights and freedoms which may be affected by the processing of personal data in a modern society. The convention, also known as Convention 108, has been ratified by more than 40 Member States of the Council of Europe, including all EU Member States. Convention 108 will be amended by its Protocol (CETS No 223) upon its entry into force.

Directive 95/46/EC, which was the predecessor to the GDPR, was based on the principles of Convention 108, but specified and developed them in many ways. It aimed to provide a high level of protection and a free flow of personal data in the EU. When the Commission made the proposal for this directive in the early 1990s, it stated that Community institutions and bodies should be covered by similar legal safeguards, thus enabling them to take part in a free flow of personal data, subject to equivalent rules of protection. However, until the adoption of Article 286 TEC, a legal basis for such an arrangement was lacking.

On 6 April 2016, the EU agreed to a major reform of its data protection framework, adopting

the GDPR to replace the old Directive. The GDPR is an essential step forward in strengthening citizens' fundamental rights in the digital age. It focuses on reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards.

In addition to this, the GDPR increases the territorial scope of the EU's data protection rules, introduces administrative fines, strengthens the conditions for consent and gives people more control over their personal data, in particular making it easier to access.

The Treaty of Lisbon enhances the protection of fundamental rights in different ways. Respect for private and family life and protection of personal data are treated as separate fundamental rights in Articles 7 and 8 of the Charter. This is legally binding, both for the institutions and bodies, and for the EU Member States when they apply Union law. Data protection is also dealt with as a horizontal subject in Article 16 TFEU. This clearly indicates that data protection is regarded as a basic ingredient of *good governance*. Independent supervision is an essential element of this protection.

Regulation (EC) No 45/2001

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

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

Regulation (EU) No 2018/1725

According to Article 2(1), this Regulation applies to the *processing of personal data by all Union institutions and bodies as of 11 December 2018*. However, it will only apply to the processing of personal data by Eurojust from 12 December 2019 and it does not apply to the processing of operational personal data by Europol and the European Public Prosecutor's Office, nor to the processing of personal data as part of activities referred to in Articles 42(1), 43 and 44 TEU, such as activities carried out within the framework of the common security and defence policy. In addition, only Article 3 and Chapter IX of the Regulation apply to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities of judicial cooperation in criminal matters or police cooperation.

The definitions and the substance of the Regulation closely follow the approach of the GDPR. It could be said that Regulation (EU) 2018/1725 is the implementation of the GDPR at EU institution level. The structure of Regulation 2018/1725 should be understood as equivalent to the structure of the GDPR and whenever its provisions follow the GDPR they should be interpreted homogeneously. This means that the Regulation deals with general principles like fair and lawful processing, proportionality and compatible use, consent, including special

conditions for children, special categories of sensitive data, as well as transparency, information and access to personal data and rights of the data subject. It addresses the obligations of controllers, joint controllers and processors, supervision, enforcement, remedies, liabilities and penalties. A specific section deals with the protection of personal data and privacy in the context of electronic communications. This section is the implementation for EU institutions and bodies of the Directive 2002/58/EC on privacy and electronic communications.

Regulation 45/2001 introduced the obligation for EU institutions and bodies to appoint at least one person as data protection officer (DPO) and Regulation 2018/1725 reaffirms this. These officers are tasked with ensuring the internal application of the provisions of the Regulation, including the proper notification of processing operations, in an independent manner. All institutions and most bodies now have these officers, and in some cases have done for many years. These officers are often in a better position to advise or to intervene at an early stage and to help to develop good practice. Since the DPO has the formal duty to cooperate with the EDPS, this is a very important and highly appreciated network to work with and to develop further (see section 6.2.1).

Tasks and powers of the EDPS

The tasks and powers of the EDPS were clearly described in Chapter V, in particular in Articles 41, 46 and 47, of Regulation 45/2001. This was replaced by Chapter VI and Articles 52, 57 and 58 of Regulation 2018/1725 (see Annex B), both in general and in specific terms. Article 41 of Regulation 45/2001 (Article 52 of Regulation 2018/1725) lays down the general mission of the EDPS — to ensure that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, with respect to the processing of personal data are respected by EU institutions and bodies. Moreover, it sets out some broad lines for specific elements of this mission. These general responsibilities are developed and specified in Articles 46 and 47 of Regulation 45/2001 and Articles 57 and 58 of Regulation 2018/1725 with a detailed list of tasks and powers.

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

Some tasks are of a special nature. These include the task of advising the Commission and other EU institutions about new legislation — mirrored in Article 28(2) of Regulation 45/2001 and Article 42 of Regulation 2018/1725, setting out a formal obligation for the Commission to consult the EDPS when it adopts a legislative proposal relating to the protection of personal data — as well as draft implementing or delegated acts and measures related to international agreements. This is a strategic task that allows the EDPS to look at privacy implications at an early stage and to discuss possible alternative approaches. In addition, in accordance with Article 42(2) of Regulation 2018/1725, the European Commission may consult the European Data Protection Board (EDPB), established to advise the European Commission and to develop harmonised policies under the GDPR, on proposals which are of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. In such cases, the EDPB and the EDPS coordinate their work with a view to issuing a joint Opinion.

Another important task performed by the EDPS is intervening in direct actions brought before the Court of Justice and responding to invitations from the Court to answer questions or provide information on the basis of Article 24 of the Statute of the Court in other cases. Oral pleadings by the EDPS are usually available on our website. Since December 2015, the EDPS has

been involved in a number of high-profile cases, including:

- Case C-615/13P *Client Earth and Pan Europe v EFSA*
- Case C-362/14 *Schrems v Data Protection Commissioner* (see section 5.2.3)
- Opinion 1/15 EU-Canada PNR agreement (section 5.2.4)
- Joint hearing in Case C-623/17 (Privacy International) with Joined Cases C-511/18 and C-512/18 (La Quadrature du Net and Others) and Case C-520/18 (Ordre des barreaux francophones et germanophone and Others)

The duty to cooperate with national supervisory authorities and supervisory bodies in the former *third pillar* is also of strategic importance. Cooperation with supervisory bodies in the former *third pillar* allows the EDPS to observe developments in that context and to contribute to a more coherent and consistent framework for the protection of personal data, regardless of the *pillar* or the specific context involved. Under the previous legal framework, there was no single coherent model for coordinated supervision. Article 62 of Regulation 2018/1725 now allows for the implementation of one single model for coordinated supervision of large scale information systems and of Union bodies, offices or agencies by the EDPS and national supervisory authorities.

ANNEX B - EXTRACT FROM REGULATION (EU) 2018/1725

Article 41 - Information and consultation

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

Article 42 - Legislative consultation

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

Article 52 - European data protection supervisor

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

Article 57 - Tasks

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

Article 58 — Powers

1. The European Data Protection Supervisor shall have the following investigative powers:
   a. to order the controller and the processor to provide any information it requires for the performance of his or her tasks;
   b. to carry out investigations in the form of data protection audits;
   c. to notify the controller or the processor of an alleged infringement of this Regulation;

d. to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of his or her tasks;
e. to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law.

2. The European Data Protection Supervisor shall have the following corrective powers:
a. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
b. to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
c. to refer matters to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;
d. to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
e. to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
f. to order the controller to communicate a personal data breach to the data subject;
g. to impose a temporary or definitive limitation including a ban on processing;
h. to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;
i. to impose an administrative fine pursuant to Article 66 in the case of non-compliance by a Union institution or body with one of the measures referred to in points (d) to (h) and (j) of this paragraph, depending on the circumstances of each individual case;
j. to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.

3. The European Data Protection Supervisor shall have the following authorisation and advisory powers:
a. to advise data subjects in the exercise of their rights;
b. to advise the controller in accordance with the prior consultation procedure referred to in Article 40, and in accordance with Article 41(2);
c. to issue, on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data;
d. to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 48(2);
e to authorise contractual clauses referred to in point (a) of Article 48(3);
f. to authorise administrative arrangements referred to in point (b) of Article 48(3);
g. to authorise processing operations pursuant to implementing acts adopted under Article 40(4).

4. The European Data Protection Supervisor shall have the power to refer the matter to the Court of Justice under the conditions provided for in the Treaties and to intervene in actions brought before the Court of Justice.

5. The exercise of the powers conferred on the European Data Protection Supervisor pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedies and due process, set out in Union law.

ANNEX C - THE ROLE OF THE EDPS

Supervision and enforcement

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

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

Policy and consultation

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

- **Informal Comments:** In line with established practice, the Commission is encouraged to consult the EDPS informally before adopting a proposal with implications for data protection (Recital 60 of Regulation 2018/1725). This allows us to provide them with input at an early stage of the legislative process, usually in the form of informal comments, which are not published.
- **Opinions:** Our formal Opinions are available on our website and summaries in all official languages are published in the Official

Journal of the EU. We use them to highlight our main data protection concerns and recommendations on legislative proposals or other measures. They are issued on our own initiative or on request and 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 through interventions in support of one of the parties in a case or at the invitation of the Courts (see Annex A).
- **International Cooperation, including with national DPAs:** We cooperate with national DPAs through the EDPB. We also work with national DPAs to ensure a consistent and coordinated approach to the supervision of a number of EU databases. We cooperate with international organisations to promote a data protection culture and we closely follow relevant developments at the OECD, Council of Europe and other fora. The EDPS is also an active member of the ICDPCC.

Monitoring technological developments

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, the data protection Directive for the police and justice sectors and Regulation 2018/1725 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 that incorporate privacy concerns and to encourage engineers to build privacy mechanisms into internet services, standards and apps.
- **Establishing the state of the art in data protection by design:** With the GDPR and Regulation 2018/1725 now fully applicable, it has become a legal obligation for all controllers to take account of the state of the art in data protection friendly technology when designing, maintaining and operating IT systems for the processing of personal data. In order to ensure consistent application of this rule across the entire EU, DPAs must work together to establish a common understanding of the state of the art and its development.

ANNEX D - LIST OF OPINIONS AND FORMAL COMMENTS ON LEGISLATIVE PROPOSALS

All Opinions, Formal Comments and other documents issued by the EDPS between 1 January 2015 and 30 September 2019 are listed below. Please refer to the EDPS website for translations and executive summaries.

2019

Opinions

- Service of documents and taking of evidence in civil or commercial matters 2018 (13 September 2019)
- EDPB-EDPS Joint Opinion on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI) (9 July 2019)
- EU-US agreement on cross-border access to electronic evidence (2 April 2019)
- Budapest Cybercrime Convention (2 April 2019)
- Combating VAT fraud (14 March 2019)

Formal comments

- Proposals on Regulations establishing the conditions for accessing other EU information systems for ETIAS purposes (15 March 2019)
- Commission proposal on preventing the dissemination of terrorist content online (13 February 2019)
- Credit servicers, credit purchasers and the recovery of collateral (25 January 2019)
- Return directive recast proposal of the new regulation (10 January 2019)

2018

Opinions

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

Formal comments

- European Border and Coast Guard (3 December 2018)
- Covered bonds and covered bonds public supervision (12 October 2018)
- Facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences (10 September 2018)

- Insurance against civil liability in respect of the use of motor vehicles (26 July 2018)
- Review of OLAF Regulation (24 July 2018)
- Migration and international protection (18 July 2018)
- Fisheries controls (18 July 2018)
- Copyright in the Digital Single Market (3 July 2018)
- Free-flow of non-personal data in the European Union (8 June 2018)
- European Labour Authority (ELA) (30 May 2018)
- Screening of foreign direct investments into the European Union (12 April 2018)
- VAT fraud and administrative cooperation (8 March 2018)
- Visa Information System (VIS) to include data on long stay visas and residence documents (9 February 2018)

2017

Opinions

- Opinion on ECRIS-TCN (12 December 2017)
- Proposal for a Regulation on integrated farm statistics (20 November 2017)
- Proposal of the 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

- Proposal for a Regulation on the European citizens' initiative (19 December 2017)
- Cybersecurity package (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)
- 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

- 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)

2016

Opinions

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

Formal comments

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

2015

Opinions

- Dissemination and use of intrusive surveillance technologies (15 December 2015)
- Meeting the challenges of Big Data (19 November 2015)
- Recommendations on the Directive for data protection in police and justice sectors (28 October 2015)
  Updated comparative table (7 December 2015)
- The use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (24 September 2015)
- Towards a new digital ethics: data, dignity and technology (11 September 2015)
- Recommendations on the EU's options for data protection reform (27 July 2015)
- EU-Switzerland agreement on the automatic exchange of tax information (8 July 2015)
- Mobile Health: Reconciling technological innovation with data protection (21 May 2015)

Formal comments

- European Commission public consultation on online platforms (16 December 2015)
- European Commission Public Consultation on Smart Borders (3 November 2015)
- EU Medicines Agencies Network Strategy to 2020 - Working together to improve health (25 March 2015)
- Exchange of information in the field of taxation (17 June 2015)
- EU-wide real-time traffic information services (21 January 2015 and 17 June 2015)

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

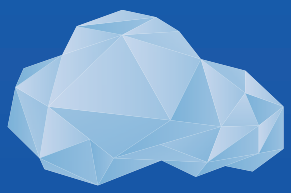
You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

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

1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1

@EU_EDPS
EDPS
European Data Protection Supervisor

Publications Office
of the European Union

ISBN 978-92-9242-450-3