EDPS

ANNUAL REPORT 2019

EUROPEAN DATA PROTECTION SUPERVISOR

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

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

The website also details a subscription feature to our newsletter.

Luxembourg: Publications Office of the European Union, 2019

Print	ISBN 978-92-9242-558-6	ISSN 1830-5474	doi:10.2804/651351	QT-AA-20-001-EN-C
PDF	ISBN 978-92-9242-559-3	ISSN 1830-9585	doi:10.2804/945	QT-AA-20-001-EN-N
HTML	ISBN 978-92-9242-557-9	ISSN 1830-9585	doi:10.2804/63038	QT-AA-20-001-EN-Q

ANNUAL REPORT 2019

European Data Protection Supervisor

Contents

TABLES AND GRAPHS

Foreword

2019 could be described as a year of transition, across Europe and the world.

It was the year the world finally woke up to the reality of the climate crisis and demanded action from governments and individuals. The EDPS contributed to the discussion, launching a debate on the role that emerging technologies can play in both exacerbating and alleviating the problem.

It was the year that Hong Kong rose up to protect itself against the dark side of technology, opening the world's eyes to the dangers of complacency and technological determinisim. Protestors' masks have become a symbol of defiance across the world against the use of surveillance techniques and the debate has taken centre stage in Europe, with EU leaders and policymakers focused on evaluating the legality and morality of the use of facial recognition technologies.

It was also a year of great change for the EU. A new Parliament, a new Commission and even a new (though very familiar!) EDPS took office, bringing with them new priorities and perspectives. With a clear focus on developing an effective response to digital challenges at the top of the EU agenda, it is clear that the EDPS and our colleagues at the European Data Protection Board (EDPB) are in for a busy few years!

With new legislation on data protection in the EU now in place, our greatest challenge moving into 2020 is to ensure that this legislation produces the promised results. This includes ensuring that new rules on ePrivacy remain firmly on the EU agenda. Awareness of the issues surrounding data protection and privacy and the importance of protecting these fundamental rights is at an all time high and we cannot allow this momentum to decline.

For the EDPS, this includes a continued effort to maintain the highest standards of data protection practice across all EU institutions, bodies, offices and

agencies. With an eye on the European Parliament elections in May 2019, the EDPS and other EU data protection authorities (DPAs) worked hard to raise awareness of the dangers of online manipulation, both within and outside the EU institutions, helping to ensure that the elections passed without incident. We followed this up with an investigation into the Parliament's use of the company NationBuilder to manage its election website, ensuring that citizens' data is adequately protected when in the hands of an EU institution.

Another EDPS investigation, into contractual agreements between the EU institutions and Microsoft, brought the issue of the EU's digital sovereignty to the fore. This is undoutedly an area that both the EDPS and the EU in general will continue to explore over the coming years, as Europe looks to develop its own unique and independent approach to the digital revolution.

Tragically, however, we will have to do this without the help of one of the data protection community's greatest advocates for the protection and promotion of human dignity.

Giovanni Buttarelli was a visonary thinker in the field of data protection and beyond, who led the EDPS as both Supervisor and Assistant Supervisor for almost ten years. His actions and achievements over the course of his career have shaped data protection across the EU and globally. This Annual Report serves as a tribute from his staff to him and his vision; of an EU that leads by example in the debate on data protection and privacy in the digital age.

Wojciech Wiewiórowski
European Data Protection Supervisor

Mission statement, values and principles

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

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

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

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

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

Core values

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

Guiding principles

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

EDPS Strategy 2015-2019

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

About the Strategy

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

The 2015-2019 strategic plan summarised:

- the major data protection and privacy challenges predicted 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.

Vision, Objectives and Actions 2015-2019

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

1 Data protection goes digital

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

(2) identifying cross-disciplinary policy solutions;

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

2 Forging global partnerships

(4) developing an ethical dimension to data protection;

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

(6) mainstreaming data protection into international policies.

3 Opening a new chapter for EU data protection

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

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

(9) facilitating responsible and informed policymaking;

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

@EU_EDPS

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

1. About the EDPS

The 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, and the EU's agency for judicial cooperation, Eurojust. The relevant legislation in this case is Regulation 2016/794, which applies to Europol, and Regulation 2018/1727, which applies to Eurojust. As for the other EU institutions and bodies, the EDPS is also responsible for supervising the processing of personal data relating to administrative activities at Europol and Eurojust, including personal data relating to their staff members, under Regulation 2018/1725. A similar, specific, data protection regime is in place for the European Public Prosecutor's Office.

1.1 SUPERVISION AND ENFORCEMENT

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

- **Prior consultations:** Under Regulation 2018/1725, EU institutions and bodies are required, in certain cases, to 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, data protection audits and investigations.
- **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 these DPOs, providing them with training and support to help them perform their role effectively.

- **Training the EU institutions and bodies:** We provide training sessions for managers and staff members of the EU institutions and bodies. These help to ensure compliance with data protection rules and respect for the rights and freedoms of individuals, and to encourage the development of a data protection culture within each institution. These training sessions focus on helping institutions to go beyond compliance and demonstrate accountability.

1.2 POLICY AND CONSULTATION

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

- **Informal Comments:** In line with established practice, the Commission is encouraged to consult the EDPS informally before adopting a proposal with implications for data protection. This allows us to provide them with input at an early stage of the legislative process, usually in the form of informal comments, which are not published.

- **Opinions:** Our formal Opinions are available on our website and 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 chapter 4).

- **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 Organisation for Economic Cooperation and Development (OECD), Council of Europe and other fora. The EDPS is also an active member of the Global Privacy Assembly (formerly known as the International Conference of Data Protection and Privacy Commissioners).

1.3 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.

2. 2019 - An Overview

In 2019 we reached the end of a five-year supervisory mandate at the EDPS, which began with the appointment of Giovanni Buttarelli and Wojciech Wiewiórowski as EDPS and Assistant Supervisor respectively in December 2014. At the start of this mandate, we published the EDPS Strategy 2015-2019, which has served as the inspiration for our work over the past five years.

Our work in 2019 therefore focused on consolidating the achievements of the preceding years, assessing the progress made and starting to define priorities for the future.

Sadly, in August 2019, EDPS Giovanni Buttarelli passed away. He leaves behind a legacy that will shape not only the future of the EDPS, but the future of data protection globally.

In December 2019, former Assistant Supervisor Wojciech Wiewiórowski was appointed by the Council and the European Parliament as the new EDPS and began work on defining a new EDPS Strategy for the 2019-2024 mandate. In accordance with the new rules on data protection in the EU institutions, the position of Assistant Supervisor was abolished.

The new EDPS Strategy will be published in March 2020 and will define our priorities and objectives for the years to come.

2.1 A NEW CHAPTER FOR DATA PROTECTION

In 2019, the EU's new data protection framework celebrated its first anniversary. One of the three objectives set out in our Strategy 2015-2019 was to open a new chapter for EU data protection. Our work in 2019 therefore focused on putting the new rules into practice.

In the case of the General Data Protection Regulation (GDPR), this meant continuing to provide and support the secretariat of the European Data Protection Board (EDPB), while also contributing fully as a member of the EDPB. Made up of the 28 EU Member State data protection authorities (DPAs) and the EDPS, the EDPB is responsible for ensuring the consistent implementation of the GDPR across the EU.

As a member of the EDPB, we contributed to several initiatives in 2019. This included working with the EDPB to produce the first joint EDPS and EDPB Opinion, on the processing of patient data through the EU's eHealth network (see section 3.2.4), as well as issuing joint advice to the European Parliament on the EU response to the US CLOUD Act, which gives US law enforcement authorities the power to request the disclosure of data by US service providers, regardless of where in the world this data is stored (see section 3.1.8).

December 2019 marked a year since the new data protection rules for the EU institutions - set out in Regulation (EU) 2018/1725 - came into force. Our focus over the year was therefore on ensuring that the EU institutions were able to effectively implement these rules. This involved continuing to work closely with the Data Protection Officers (DPOs) in the EU institutions to assess the progress made and discuss how to overcome any of challenges encountered (see section 3.2.1), as well as continuing our programme of data protection training activities for EU institution employees (see section 3.2.2).

In addition to this, we also stepped up our enforcement activities, making use of the powers granted to the EDPS under the new Regulation. In June 2019, for example, we announced the results of our first round of remote inspections of EU institution websites, highlighting several areas in which the EU institutions concerned needed to improve (see section 3.2.8).

One area in which we were particularly active over the course of 2019 was in conducting investigations into the data processing activities of the EU institutions. The EDPS launched four investigations in 2019, addressing a variety of issues (see section 3.2.5). Our aim is to ensure that these investigations leave a lasting, positive impact, strengthening cooperation between the EDPS and the institutions concerned, improving the data protection practices of the EU institutions and ensuring the highest levels of protection for all individuals.

Our investigation into the use of Microsoft products and services by EU institutions is a particularly good example of this, having resulted in the establishment of The Hague Forum. Set to meet for the second time in early 2020, the Forum provides a platform for discussion on both how to take back control over the IT services and products offered by the big IT service providers and the need to collectively create standard

contracts instead of accepting the terms and conditions as they are written by these providers (see section 3.2.4).

New legislation is also in place for two of the EU's law enforcement agencies. The EDPS is now well established as the data protection supervisor for operational activities at Europol, the EU body responsible for supporting the law enforcement authorities of the Member States in the fight against serious international crime and terrorism (see section 3.2.11). In late 2019 we also took over similar responsibilities at Eurojust, the EU agency responsible for supporting and improving coordination and cooperation between the competent judicial authorities in the EU Member States on matters relating to serious organised crime (see section 3.2.12).

With public security certain to remain an important policy concern for the EU over the coming years, we are determined to ensure that the EU is able to achieve increased security without applying any undue restriction to individual data protection rights. Our roles at Europol and Eurojust therefore focus on ensuring increased operational effectiveness while ensuring that fundamental rights, including the rights to data protection and privacy, are adequately protected.

2.2 PROVIDING GUIDANCE AND ADVICE

Improving the security of EU borders is a priority for the EU legislator and will remain so over the coming years. The EDPS therefore continues to provide advice and guidance to the European Commission, the European Parliament and the Council on new initiatives in this area, while also working with national DPAs and EU institutions to ensure the continued security of EU information systems.

While we recognise the need for greater EU security, this should not come at the expense of data protection and privacy. EDPS Opinions on proposals such as an EU-US agreement on cross-border access to electronic evidence (see section 3.1.8) and European Production and Preservation Orders for electronic evidence in criminal matters (see section 3.1.5), all aim to ensure that both the personal data rights of the individuals concerned and EU borders are protected.

We also continued our close cooperation with DPAs to ensure effective and coordinated supervision of the EU's large-scale IT databases, used to support EU policies on asylum, border management, police cooperation and migration (see sections 3.1.1 and 3.1.2).

In addition to this, we have endeavoured to provide policymakers with tools to help assess the compliance of proposed EU measures that would impact the fundamental rights to privacy and the protection of personal data with the Charter of Fundamental Rights. On 19 December 2019, we published our Guidelines on assessing proportionality. Combined with our Necessity Toolkit, these Guidelines provide practical guidance for policymakers helping to simplify the challenges they face in assessing the necessity and proportionality of certain policy proposals and therefore ensure that fundamental rights are adequately protected (see section 3.2.7).

Our guidance is not limited to policymakers, however. In 2019 we also issued Guidelines on the roles and concepts of controller, processor and joint controllership, in an attempt to clarify these concepts and help those working in the EU institutions to better understand their roles and comply with data protection rules (see section 3.2.7).

In addition to this, a significant focus of our work in 2019 was on developing and sharing technological expertise. With so much of our lives now reliant on the use of technology, this expertise is essential to ensuring effective data protection and the EDPS has consistently aimed to take the lead in sharing helpful analyses of new technological developments (see section 3.2.9).

Through our TechDispatch publication, launched in July 2019, we contribute to the ongoing discussion on new technologies and data protection. Focusing on a different emerging technology each issue, we aim to provide information on the technology itself, an assessment of its possible impact on privacy and data protection and links to further reading on the topic.

Following the first round of our remote inspections of EU institution websites, we also took the step of publicly sharing the Website Evidence Collector (WEC) tool developed by the EDPS. The tool is available on the EDPS website and on the code collaboration platform GitHub as free software and allows for the collection of automated evidence of personal data processing. By sharing the WEC, we hope to provide DPAs, privacy professionals, data controllers and web developers with the tools to carry out their own website inspections.

Lastly, we continued our work on developing the Internet Privacy Engineering Network (IPEN), which brings together experts from a range of different areas to encourage the development of engineering solutions to privacy problems. Five years on from when it was first established, IPEN is now in a position to move beyond more general discussion of the issues surrounding privacy engineering and towards a more targeted

approach, focused on developing practical solutions to privacy engineering problems (see section 3.2.10).

2.3 AN INTERNATIONAL APPROACH TO DATA PROTECTION

Over the past five years, the EDPS has dedicated significant time and energy to the development of greater data protection convergence globally. While data flows internationally, across borders, data protection rules are still decided on a largely national, and at best regional, basis.

Throughout 2019 we have therefore continued to work with our regional and international partners to mainstream data protection into international agreements and ensure consistent protection of personal data worldwide. In particular, we have worked closely with the EDPB on the topic of international data transfers, participating in the review of the Privacy Shield agreement for data transfers between the EU and the US, as well as the EDPB contribution to the hearing on the Schrems case at the EU Court of Justice, focused on the legality of standard contractual clauses for data transfers (see section 3.3.1).

We also persisted in the pursuit of our goal to foster global debate on digital ethics. Building on the success of the 2018 International Conference of Data Protection and Privacy Commissioners, co-hosted by the EDPS in Brussels, in 2019 we sought to ensure that the debate on ethics in the digital sphere continued to move forward. We therefore launched a series of webinars, which we published in the form of a podcast on our website. Each webinar focused on a specific area of concern identified during the conference, allowing us to explore the topic in more detail (see section 3.3.2).

Discussion on digital ethics also continued at the 2019 International Conference, both through the working group on Artificial Intelligence, Ethics and Data Protection, and through the organisation of an EDPS side event, focused on the environmental impact of digital technologies (see section 3.3.2).

2.4 INTERNAL ADMINISTRATION

The size and responsibilities of the EDPS continue to increase. A priority for the EDPS Human Resources, Budget and Administration (HRBA) unit in 2019 was therefore to ensure that the EDPS has the appropriate resources to carry out its tasks (see section 6.2). This included the completion of a competition for experts in the area of data protection and the publication of a reserve list from which to draw new staff members, as well as stepping up efforts to maximise and acquire office space to accommodate our growing population.

We also endeavoured to improve learning and development opportunities for existing staff members, in particular through the launch of an internal coaching initiative. In addition, significant progress was made in the areas of finance and procurement, with the introduction of more efficient processes for financial operations; this will continue to be an area to work on in 2020.

As we begin the new mandate, our focus will be on continuing to improve the efficiency of administrative processes, in order to ensure that the EDPS is well equipped to respond to new challenges in data protection.

2.5 COMMUNICATING DATA PROTECTION

The reach and influence of EDPS communications is constantly expanding (see section 6.1). Effective communication is vitally important in ensuring that information on EDPS activities reaches the relevant external audience.

With public interest and engagement with data protection increasing, our communication efforts in 2019 aimed to build on successes of previous years and reinforce our status as a respected, international leader in the data protection field. This involved sustained efforts in several areas, including online media, events and publications and external relations with press and stakeholders.

With a new mandate now underway, our focus for the coming year will be on continuing to develop our communications tools to support the successful implementation of the new Strategy, to be published in March 2020.

2.6 KEY PERFORMANCE INDICATORS 2019

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

The KPI scoreboard below contains a brief description of each KPI and the results on 31 December 2019. In most cases, these results are measured against initial targets.

In 2019, we met or surpassed - in some cases significantly - the targets set in six out of the eight KPIs, with KPI 2 just falling short of the set target.

These results reflect the positive outcome we have had in implementing relevant strategic objectives during the last year of the 2015-2019 Strategy.

Finally, KPI 7 cannot be measured in 2019, as the staff survey is conducted only once every two years.

KEY PERFORMANCE INDICATORS		RESULTS AT 31.12.2019	TARGET 2019
Objective 1 - Data Protection goes digital			
KPI 1 Internal Indicator	Number of initiatives promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	9 initiatives	9 initiatives
KPI 2 Internal & External Indicator	Number of activities focused on cross-disciplinary policy solutions (internal & external)	7 activities	8 activities
Objective 2 - Forging global partnerships			
KPI 3 Internal Indicator	Number of cases dealt with at international level (EDPB, CoE, OECD, GPEN, International Conferences) for which EDPS has provided a substantial written contribution	62 cases	10 cases
Objective 3 – Opening a new chapter for EU Data Protection			
KPI 4 External Indicator	Number of opinions/comments issued in response to consultation requests (COM, EP, Council, DPAs...)	26 consultations	10 consultations
KPI 5 External Indicator	Level of satisfaction of DPOs/DPCs/controllers on cooperation with EDPS and guidance, including satisfaction of data subjects as to training	90%	70%
Enablers – Communication and management of resources			
KPI 6 External Indicator	Number of followers on the EDPS social media accounts (Twitter, LinkedIn, YouTube)	40421 (L: 20357, T: 18424, Y: 1640)	Number of followers of previous year + 10%
KPI 7 Internal Indicator	Level of Staff satisfaction	N/A	75%
KPI 8 Internal Indicator	Budget implementation	91.69%	90%

Figure 1. EDPS KPI analysis table

3. 2019 Highlights

2019 might be described as a year of transition for the EDPS, as one mandate came to an end and a new one began. However, though our focus may have been on the consolidation of achievements and progress made over the preceeding years, we continued to make significant contributions to ensuring effective data protection in the EU and globally.

Protecting EU security and borders remains a significant priority for the EU legislator and we continued to contribute fully to the discussion on how to do so without compromising the fundamental rights to data protection and privacy.

With the new EU data protection framework now in place, one of our main priorities for 2019 was to ensure that these new rules were effectively implemented within the EU institutions. This involved not only working with our partners in the EU institutions to increase awareness and provide guidance, but also exercising our powers to enforce the new rules.

Our efforts to develop our relationships with international partners also continued. This included strengthening our relationship with the European Data Protection Board (EDPB), as well as with international organisations, in an effort to work towards increased international convergence on data protection rules and principles.

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

As we begin a new mandate, under new EDPS Wojciech Wiewiórowski, we look forward to building on the achievements of the past five years as well as establishing new priorities and objectives to guide our work. With the importance of data protection now firmly established on the international agenda, we have no doubt that the EDPS will continue to serve as an important point of reference for all things data protection in the EU.

3.1 SECURITY AND EU BORDERS

The EDPS strongly supports the EU legislator's attempts to increase EU security and border management. Terrorist attacks, the migration crisis and the development of increasingly sophisticated new technologies are contemporary realities to which the EU must adapt to ensure that EU processes and policies remain up to the task of guaranteeing safe and secure borders.

However, increased security cannot come at the expense of the fundamental rights guaranteed under the EU Charter. In fact, increased security depends on ensuring that individuals retain their fundamental rights and freedoms.

To help the EU legislator make informed decisions on EU security and border policy, the EDPS provides appropriate legal advice, guidance and recommendations on new policy proposals. We also work in close cooperation with our fellow data protection authorities (DPAs) to ensure that the tools used to implement EU border policy continue to function to the highest standards of EU data protection law.

3.1.1 Effective supervision of large-scale IT systems

The European Union operates several large-scale IT databases that are used to support EU policies on asylum, border management, police cooperation and migration. Through the databases, national authorities, as well as some EU bodies, are able to exchange information relating to borders, migration, customs and police investigations.

The EDPS is responsible for supervising the processing of personal data in the central units of the databases, the majority of which are hosted by the EU's Agency for

the operational management of large-scale IT systems in the area of freedom, security and justice (euLISA). The national DPAs are responsible for supervising how national authorities use these systems. This means that while the supervisory tasks of the EDPS relate to the management of the IT systems, those of the EU DPAs relate to the use of these systems by their respective national authorities. The relevant supervisory authority therefore depends on who processes the data.

As part of our supervisory responsibilities, the EDPS carries out periodic inspections of the central databases. Our inspections focus on the security and management of the systems, while the national authorities are responsible for ensuring the accuracy of the information registered in the systems. Carrying out inspections is a way for us to monitor data protection compliance, but also to work directly with eu-LISA to improve accountability in the management of these databases.

In December 2019, we carried out an on-site inspection, at euLISA premises in Strasbourg, of Eurodac, the EU fingerprint database for identifying asylum seekers and irregular border-crossings. In addition to following-up on our last Eurodac inspection, which took place in 2016, our aim was to assess the overall operational management of the system and the security measures applied by euLISA, as well as the processes in place to manage security incidents and personal data breaches. We will share our report and recommendations with eu-LISA, the European Parliament, the Council, the European Commission, and national DPAs in 2020, and follow up with them where appropriate.

As is legally required, we sent our report on the 2018 SIS and VIS inspection to euLISA for their comments. We will also share the final report with the European Parliament, the Council, the European Commission and national DPAs.

3.1.2 Coordinated supervision of large-scale IT systems

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

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

In 2019, the SCGs for Eurodac, the Schengen Information System (SIS) and the Visa Information System (VIS) met twice, in June and November, while the SCG for the Customs Information System (CIS) met once, in May. The results of these meetings are published on their respective webpages on the EDPS website. The meetings continue to provide a valuable forum for cooperation between the Member State DPAs and the EDPS, while also respecting the role and competences of each.

The SCGs will meet again in 2020 as part of our ongoing commitment to ensuring effective, efficient, coordinated and consistent supervision of these important databases.

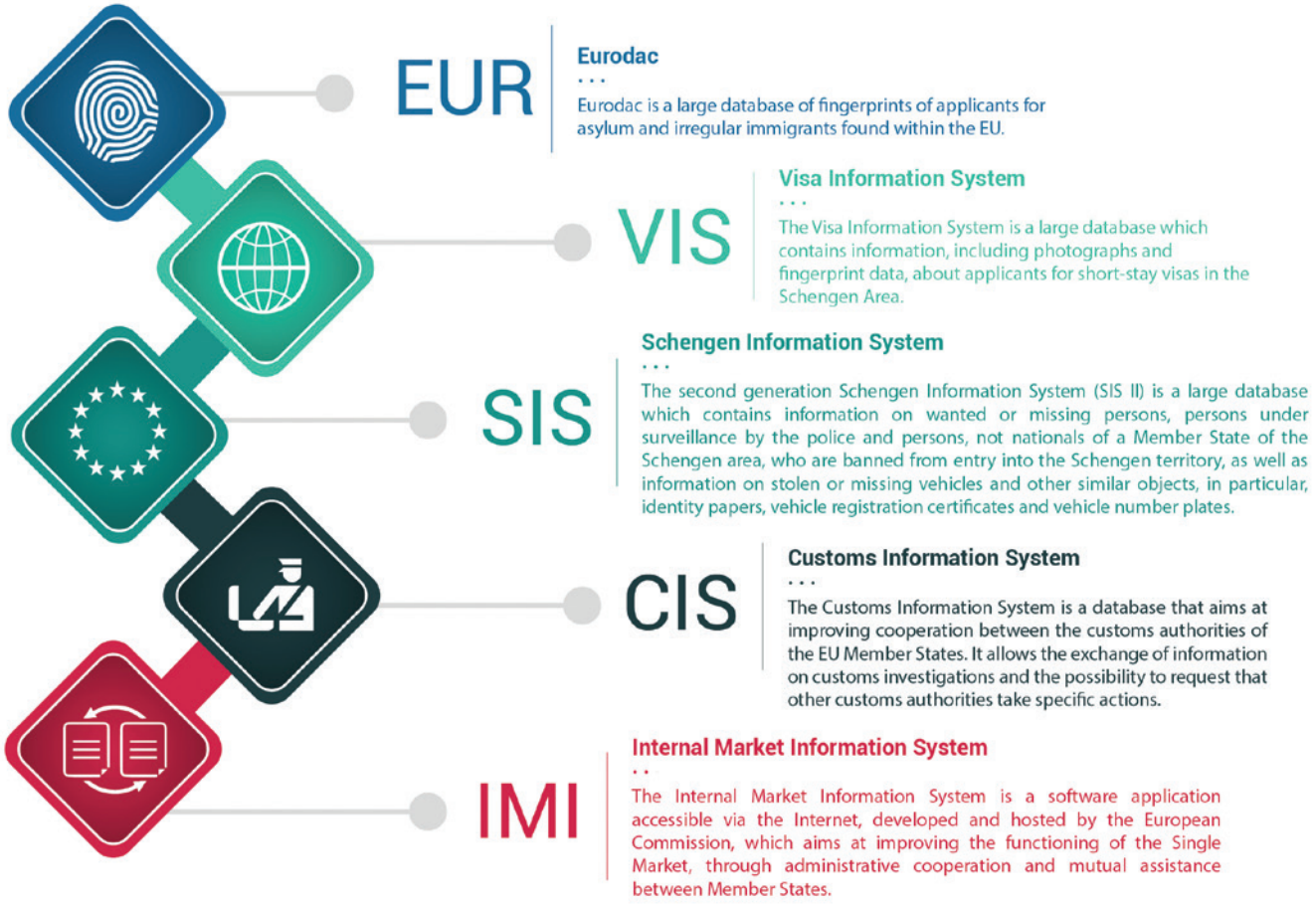
3.1.3 The future of coordinated supervision

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 becomes applicable.

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

To put the new model of coordinated supervision envisaged by the legislator into practice, the EDPB changed its rules of procedure in November 2019, in order to establish a Coordinated Supervision Committee (CSC). The CSC held its first meeting on 3 December 2019, in which it adopted its own Rules of Procedure and appointed a coordinator.



3.1.4 Observing Schengen

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

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

With our experience supervising the central units of the SIS and VIS (see section 3.1.3), the EDPS is able to offer a different and complementary perspective on the SCHEVAL process. This is of clear benefit in the supervision, enforcement and promotion of data protection in this highly sensitive area. Our input is also helpful on a linguistic level, as the international composition of our institution means that the EDPS staff members taking part in the evaluation often speak the language of the country being evaluated.

The data protection aspect of the evaluation involves assessing the competent authorities' compliance with data protection rules, including the security of the SIS and VIS databases; the independence, role and powers of the national data protection authority; public awareness of Schengen; and international cooperation. During 2019 we took part in four SCHEVAL processes, acting as an observer for the evaluations of the Czech Republic, Poland, Hungary and Cyprus.

3.1.5 A pragmatic and balanced approach to e-evidence in the fight against crime

Increasingly, law enforcement authorities find themselves in a position where the information they

need is stored electronically in another State. To address this problem, the European Commission put forward two proposals in April 2018 on electronic evidence (e-evidence). These would introduce two new types of binding orders for criminal proceedings, allowing for access to data stored by service providers that may serve as evidence (Production Orders), or for the preservation of this data by service providers in anticipation of subsequent requests for access (Preservation Orders).

The proposal aims to streamline procedures within the EU, facilitating and accelerating access to cross-border data. Yet, while it is vital to ensure that law enforcement and judicial authorities have access to the necessary information and tools that are effective in the fight against terrorism and other crimes, any initiative in this field must fully respect the EU Charter of Fundamental Rights and the EU data protection framework.

On 6 November 2019, we published an Opinion on a new EU legal framework for gathering electronic evidence in cross-border cases. It provides the EU legislator with new input on the 2018 Proposals, focusing in particular on the need to ensure that all necessary safeguards are in place. This includes providing for the increased involvement of the judicial authorities in the enforcing Member State during the process of gathering cross-border electronic evidence.

In the Opinion we also call for clearer definitions of data categories in the proposed Regulation. This includes ensuring that they are consistent with existing definitions of data categories in EU law. The balance between the types of offences for which Production Orders could be issued and the categories of data concerned must also be reassessed, taking into account case law of the Court of Justice of the EU.

Since April 2018, the Council has adopted general approaches on the Proposals and the European Parliament has issued several working documents. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) published a draft report on the Proposals in December 2019, followed by a debate on the amendments. The final adoption of the report is tentatively scheduled for the beginning of 2020.

Related developments have also taken place at international level. These include the launch of negotiations with the United States on cross-border access to e-evidence (see section 3.1.8), as well as work in the Council of Europe on a Second Additional Protocol to the Cybercrime Convention (see section 3.1.7), both of which we have commented on in our Opinions.

3.1.6 Putting passengers' rights first in the transfer of PNR data to Japan

On 25 October 2019, the EDPS adopted an Opinion on the negotiating mandate of an Agreement between the EU and Japan for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crimes. PNR data is the information provided by passengers to airlines in order to make reservations and check in for a flight. It includes the dates of travel, the payment method used and passenger contact details, among other information.

The purpose of the envisaged Agreement is to lay down the legal basis and the conditions under which air carriers will be authorised to transfer to Japan the PNR data of passengers flying between the EU and Japan. This must be done in compliance with EU law, including the Charter of Fundamental Rights of the EU. If an Agreement is reached before the Olympics takes place in Japan in summer 2020, for example, it will apply to all individuals from the EU travelling to Japan to watch and take part in the Games.

The Commission has made an effort to align the proposed negotiating mandate as much as possible with the 2017 EU Court of Justice Opinion on the EU-Canada PNR Agreement, in which several of the proposed provisions were found to not be compatible with EU fundamental rights. Nevertheless, given the impact of the envisaged agreement on the fundamental rights of a very large number of individuals not implicated in a criminal activity, the EDPS made a number of recommendations. These are aimed at ensuring the proportionality of the PNR system and limiting any interference with the rights of individuals to what is strictly necessary and justified by the general interest of the Union.

Some of our specific recommendations concerned the risk of indirectly revealing special categories of data about air passengers and the risk of re-identification of individuals after the anonymisation of the PNR data relating to them. We also recommended adding clauses allowing for suspension of the Agreement if its rules are breached, as well as for its termination if non-compliance is serious and persistent.

To avoid possible confusion, our Opinion clarifies that the Commission adequacy decision on Japan adopted in January 2019 is not applicable in the case of PNR transfers.

We expect to be further consulted on the draft Agreement once it is finalised.

3.1.7 Supporting greater international cooperation on cybercrime

At the request of the European Commission, on 2 April 2019 the EDPS published an Opinion on the Commission's Recommendation for a Council Decision that would authorise the Commission to participate in negotiations towards a Second Additional Protocol to the Budapest Cybercrime Convention.

Negotiations on the new Protocol aim to improve cooperation in the collection of electronic evidence in criminal matters. The planned additions also concern direct cross-border cooperation between law enforcement authorities and service providers, including direct cross-border access to data, which is a significant development.

The EDPS has consistently pushed for sustainable arrangements for personal data sharing with non-EU countries for law enforcement. We supported the Commission's participation in negotiations to ensure the compatibility of the new Protocol with EU law. In addition to several specific recommendations, we advocated ensuring the mandatory nature of the agreement, which should include detailed safeguards, especially in terms of purpose limitation. This principle is particularly important as not all parties to the Protocol operate under the same data protection frameworks.

In June 2019, the Council adopted the Decision, giving the Commission the mandate to participate in the negotiations. Some provisions of the draft Protocol were subsequently published in October 2019 and we provided input through the EDPB. This involved responding both to the consultation itself and to the opinion of the consultative committee of the convention for the protection of individuals with regard to the automatic processing of personal data, in which the EDPS participates as an observer. We also attended the Octopus Conference organised in November 2019, where these provisions were discussed with stakeholders.

We expect to be consulted again, particularly on the draft provisions of the Protocol related to data protection, which are still being prepared, and on the final text of the draft Protocol, when it is ready.

3.1.8 Cross-border access to electronic evidence

To make our justice system as effective as possible, EU law enforcement authorities need to be able to work and exchange information with partners outside the EU. However, it is important to ensure that the fundamental rights of people within the EU remain protected when doing so.

Negotiating an EU-US agreement on access to electronic evidence

On 2 April 2019 we issued an Opinion on a Recommendation for a Council Decision that would authorise negotiations on an EU-US agreement on cross-border access to electronic evidence as part of judicial cooperation in criminal matters.

The proposed agreement would establish common rules on direct cooperation between law enforcement authorities and service providers in the EU and the US and address any conflicts between our laws on obtaining content and non-content data.

Our Opinion provided constructive and objective advice on the negotiating mandate of an EU-US agreement to lay down common rules on cross-border access to electronic evidence. We welcomed confirmation that the EU-US Umbrella Agreement would be referenced in the proposed agreement, and therefore fully applicable, in addition to other safeguards.

More specifically, we proposed that judicial authorities designated by the other Party to the agreement be involved as early as possible in the process of gathering electronic evidence. This would give these authorities the opportunity to review the compliance of any requests for evidence with fundamental rights, and to raise grounds for refusal if appropriate. We also recommended adding Article 16 of the Treaty on the Functioning of the EU, which establishes the fundamental right to the protection of personal data, as a substantive legal basis of the Council Decision.

@EU_EDPS

#EDPS issues Opinion with constructive and objective advice on the negotiating mandate of an agreement between the EU and the USA to lay down common rules on cross-border access to #electronicevidence for #judicial cooperation in criminal matters europa.eu/!CM79XF

The EDPS remains available to provide further advice to the Commission during the negotiations, as needed. We look forward to being consulted on the final text of the draft agreement when it is ready.

EDPS and EDPB advise European Parliament on US CLOUD Act

The US CLOUD Act gives US law enforcement authorities the power to request the disclosure of data by US service providers, regardless of where in the world this data is stored. Mindful of the possible implications of the Act for EU citizens, the European Parliament's LIBE Committee wrote to both the EDPS and the EDPB requesting a legal assessment. Specifically, LIBE asked us to assess the impact of the US CLOUD Act on the EU's legal framework for data protection and the mandate for negotiating an EU-US agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters.

On 10 July 2019, the EDPB and the EDPS issued a joint response. This response outlined the opinion of both the EDPS and the EDPB that a comprehensive EU-US agreement on cross-border access to electronic evidence, with strong procedural safeguards for fundamental rights, would be the most appropriate way of ensuring the necessary level of protection for individuals living in the EU, as well as to provide legal certainty for businesses.

3.1.9 Preventing the dissemination of terrorist content online

Combatting online terrorist content is important for keeping the EU safe. However, this work has to be balanced with respect for fundamental rights, including data protection.

On 13 February 2019, we issued formal Comments on the European Commission proposal on the fight against dissemination of terrorist content online. The proposal outlines the responsibilities of service providers and the actions that they are required to take. Our Comments specify that these must be aligned with the fundamental rights to privacy and data protection, enshrined in the Charter of Fundamental Rights of the EU.

To ensure compliance with the Charter, the actions that service providers have to take need to be clearly described, taking into account the principles of *quality of law* and *economic certainty*. This will also help to limit discretion and provide adequate oversight for their activities in targeting terrorist content online.

Requirements for service providers to act against terrorist content should be highly specific, taking into account how much exposure the platform has to terrorist content and the reasons behind this exposure. Importantly, these actions must not lead to the creation of a systematic or broad monitoring system.

The removal of online terrorist content based on automated tools should always be subject to human oversight, and service providers should give those affected a meaningful explanation of all measures that are used. Service providers should also give competent authorities all necessary information, so that they are able to thoroughly analyse the automated tools used and ensure that they do not produce discriminatory, untargeted, unspecific or unjustified results.

Furthermore, in line with the judgements of the Court of Justice of the European Union, we called on the Commission to reconsider the proposed obligation for service providers to retain online terrorist content and related data for at least six months for the purpose of prevention, detection, investigation or prosecution of terrorist offences.

Efforts to counter terrorist content online are a necessary part of common security policy; we therefore encourage further discussion to ensure that these efforts are balanced alongside the fundamental rights and freedoms of the EU.

3.1.10 Entering the EU under ETIAS

Citizens of over sixty non-EU countries can enter the EU Schengen Zone without a visa. The European Travel Information and Authorisation System (ETIAS), which should be in place by 2021, aims to provide the

EU with more control over how they enter. However, while the EDPS fully supports efforts to increase EU security, we have two major concerns about ETIAS, which we continue to monitor.

Firstly, the proposed system could pose a risk to EU fundamental rights and freedoms. Admission to EU territory may require additional checks at the border, which would interfere with an individual's privacy, while a decision to deny an individual entry into the Schengen area could also have negative repercussions, by placing restrictions on their ability to enjoy the right to freedom of movement. This could result in possible financial or health implications, if an individual is unable to travel to the EU to complete work commitments or to receive medical treatment that is not available in their own country, for example.

Secondly, applying data protection safeguards effectively under ETIAS is particularly challenging. This is because the data processing operations proposed involve exchanges of data between controllers who are subject to different EU data protection rules. They also involve the processing of personal data from a range of different EU databases, all established for different purposes and regulated by data protection frameworks specific to their operation. There is therefore a risk that controllers' responsibilities are watered down and that individuals will find it very difficult to exercise their data protection rights effectively.

In an effort to mitigate these risks, we have been following the data protection by design process for ETIAS, ensuring that data protection is built into the system throughout the development process. This means raising awareness of any risks to individuals, as well as supporting EU institutions in applying adequate controls to lower these risks.

With this in mind, we met with Frontex, the EU agency responsible for border management, on 25 September 2019, and with both Frontex and euLISA on 6 December 2019. As Frontex will be the main data controller for the ETIAS system, these meetings are an excellent opportunity for us to better understand how both agencies are working to implement the principle of data protection by design into the development of ETIAS. We will continue this work into 2020.

3.2. ON THE GROUND

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 data protection audits, investigations, 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, 2019 included, 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. A priority for 2019 was therefore to ensure that all EU institutions had the tools and knowledge to effectively implement accountability under the new data protection rules.

3.2.1 Working with EU institution DPOs

Each EU institution must appoint a Data Protection Officer (DPOs). Their job is to act as an independent advisor on data protection within their respective EU institution. The EDPS therefore works closely with the DPOs to ensure that they have the right tools and knowledge to perform their role.

The DPO function: EU institutions leading by example

Twice a year, DPOs from the 66 EU institutions, bodies, agencies and offices meet with the EDPS. These meetings reinforce collaboration between the DPOs and ensure that the EU institutions have the tools they need to lead by example in the application of data protection law.

With new data protection rules for the EU institutions in place by the end of 2018, our two meetings in 2019 focused on taking stock of the progress made in implementing the new rules and determining how to overcome any of the challenges encountered.

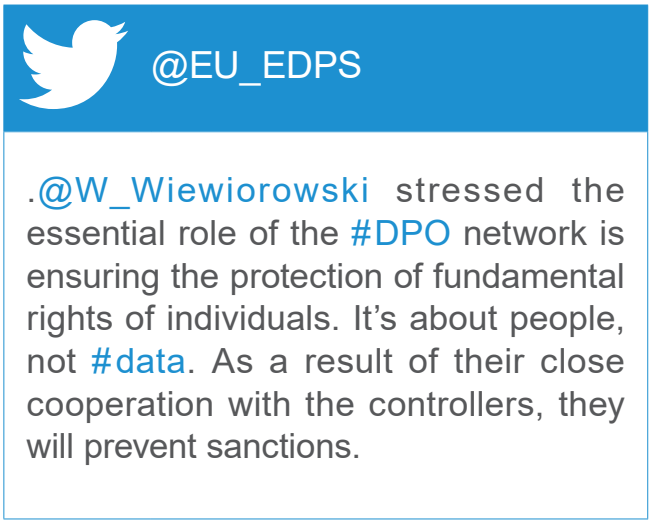
The first meeting of the year took place on 17 May 2019, hosted by the European Insurance and Occupational Pensions Authority (EIOPA) in Frankfurt. Taking place five months after Regulation 2018/1725 came into force, it was the perfect opportunity to outline the EDPS vision for monitoring the application of the new rules, while also helping DPOs to address some of

the challenges encountered in putting these rules into practice. Practical sessions on event organisation, data breach notifications (see section 3.2.3), the role of the DPO, joint controllership and procurement were organised throughout the day to help address some of the most common issues encountered by DPOs.

DPOs then met the EDPS in Florence, on 7 November 2019, at the Historical Archives of the European Union. With the location of our meeting in mind, one of the main topics up for discussion was archiving and data protection. A presentation by the Head of the Record Management sector at the EDPS provoked a lively discussion on how archivists and DPOs can work together in leading the EU institutions in their efforts to achieve accountability.

The rest of the day's activities focused on raising awareness about some of the latest developments in the data protection world. These included sessions on a recent EU Court of Justice ruling clarifying the topic of consent, on best practices to ensure data protection in mobile apps and on best practices in outsourcing, focused specifically on contracts with IT service providers.

With the new rules now in place, constructive cooperation with DPOs is now more important than ever if we are to ensure that the EU institutions are able to effectively apply data protection rules in practice.



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.

In 2018, we therefore launched several activities related to knowledge management. One of these was the creation of an internal Wiki on the new Regulation. The idea was to encourage colleagues within the EDPS 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.

However, we quickly realised that this was something that would also be useful for DPOs and Data Protection Coordinators (DPCs) working in the EU institutions. It would help them move beyond a purely compliance-based approach to data protection by giving them the tools to provide better advice in their relevant institution. As the first port of call for controllers looking for advice, DPOs and DPCs will be better able to advise colleagues if they have access to an up-to-date repository of EDPS information.

At the November 2019 DPO meeting (see section 3.2.1) we therefore opened up the Wiki to DPOs and DPCs in the EU institutions. As we move into 2020, our focus will be on ensuring that we keep the Wiki up-to-date with our evolving interpretation of the Regulation, so that all users are better informed when it comes to putting data protection rules into practice.

Quick news for DPOs

Within the EU institutions, DPOs are our main advocates for data protection compliance. They cooperate closely with us and provide advice and information to their colleagues in the EU institutions when needed. Ensuring that DPOs have access to the latest and most important news and developments in data protection is therefore vitally important.

To complement and improve our efforts to communicate through the DPO network (see section 3.2.1), we launched a monthly Newsletter aimed specifically at DPOs in September 2019. *Quick News for DPOs* provides them with a short, monthly recap of important developments in data protection, including links to new EDPS guidance, events and Opinions, and updates on European case law.

As we move into 2020, we hope that the DPO Newsletter will continue to develop into a helpful and widely-used resource for DPOs and DPCs in the EU institutions.

3.2.2 Data protection training for the EU institutions

Our work with the EU institutions does not stop with DPOs. Throughout 2017 and 2018, we organised a number of training sessions aimed at a range of different audiences. These included both managers and those directly responsible for processing personal data as part of their daily work in the EU institutions. Our aim was to ensure that they had the necessary knowledge and tools to apply the new data protection rules for the EU institutions when they came into force at the end of 2018.

@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

Our training efforts continued into 2019. With the new rules now in place, it is more important than ever to ensure that those responsible for processing personal data in the EU institutions are aware of their new obligations and know how to put the new rules into practice.

A dedicated training session on procurement for case officers at the European Parliament's Directorate General for Finance is a good example of our continued efforts to facilitate the transition to the new rules, as is the session we held for the European Commission's Directorate General for Human Resources (DG HR), one of the sectors most heavily impacted by the new rules.

3.2.3 Personal data breaches

Under Regulation 2018/1725 all European institutions, offices, bodies and agencies have a duty to report personal data breaches to the EDPS, unless a risk to the affected individuals is unlikely. 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. Similar obligations apply to Europol.

Risk assessment is a core element in preventing and responding to personal data breaches. Unlike other traditional risk assessment methodologies, the focus in a personal data breach is on evaluating the risk 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 personal data breach Guidelines aim to simplify the task by providing guidance and practical examples to assist the EU institutions in their efforts.

During 2019, the EDPS provided training and awareness raising activities for the EU institutions on personal data breach management.

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. The focus was on the challenges surrounding risk assessment, examining the legal

obligations set out in the General Data Protection Regulation and Regulation 2018/1725.

During the 45th DPO meeting, which took place on 17 May 2019 in Frankfurt (see section 3.2.1), we organised a case study on personal data breaches for all data protection officers of the European institutions, giving them a practical insight into how to deal with data breaches in their respective institutions.

In addition, the EDPS organised a dedicated personal data breach workshop with the European Commission. We developed specific training material in cooperation with the Commission and provided our guidance on key issues related to personal data breaches. Two workshops took place, on 14 and 21 June 2019, with more than 100 participants from a wide range of the European Commission's different Directorate Generals.

In November 2019, during the training days organised by the Office for administration and payment of individual entitlements (Paymaster's Office or PMO), we provided a specific training session on personal data breaches to staff working on human resources related matters from all EU institutions and agencies. More than 200 participants attended the workshop.

In 2019, the EDPS received and assessed 95 personal data breach notifications under Regulation 2018/1725. In 24 cases, the controller informed the individuals concerned.

@EU_EDPS

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

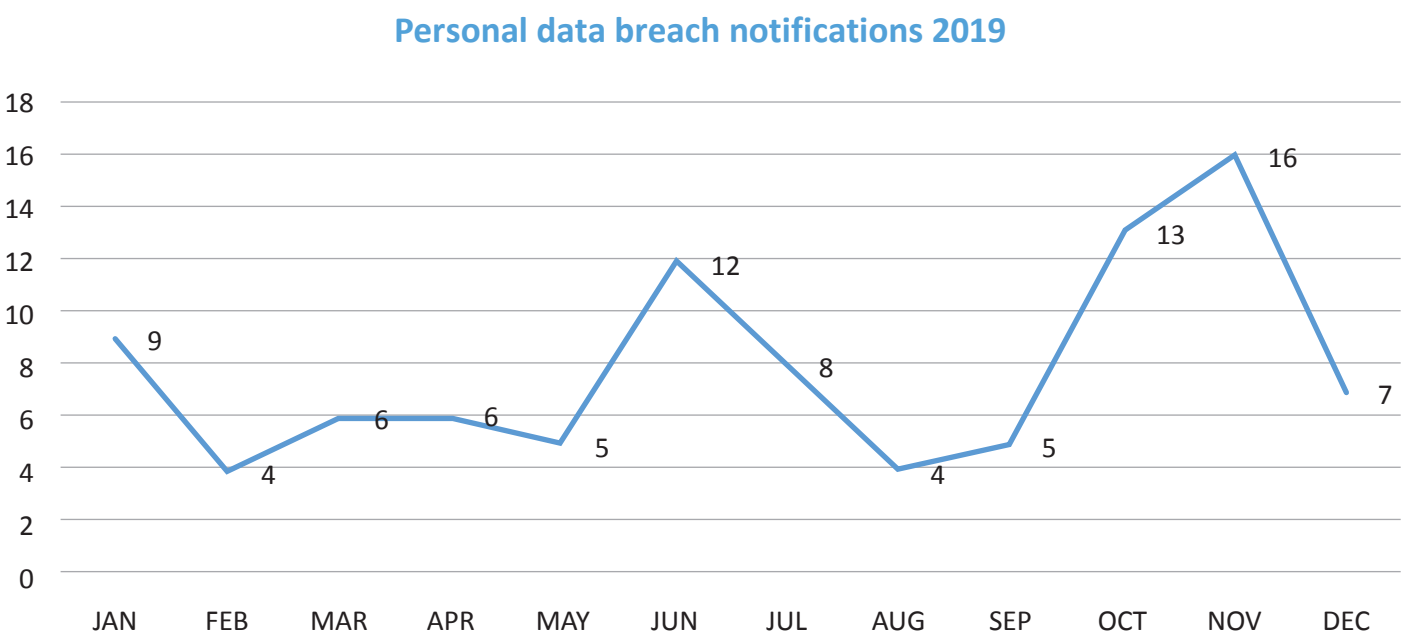


Figure 2. Number of personal data breach notifications received by the EDPS per month in 2019

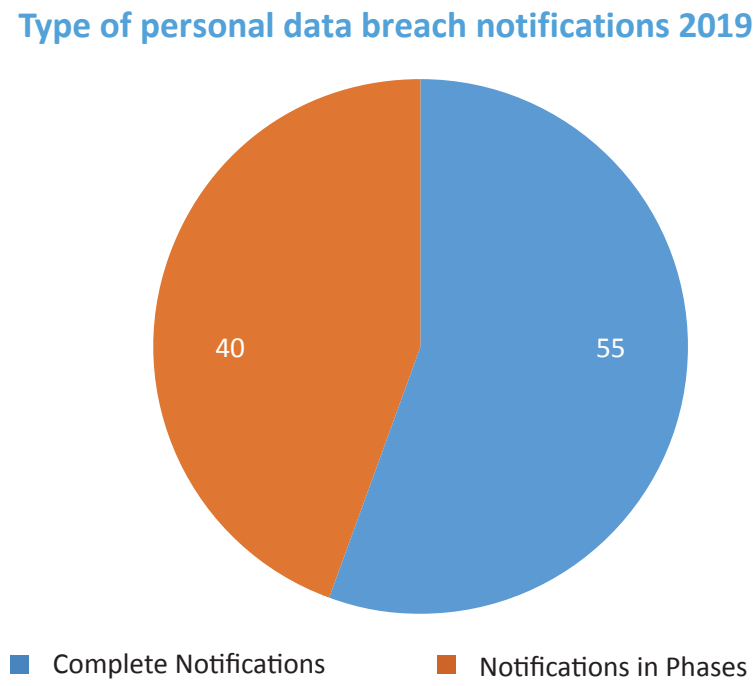


Figure 3. Type of personal data breach notifications received by the EDPS in 2019

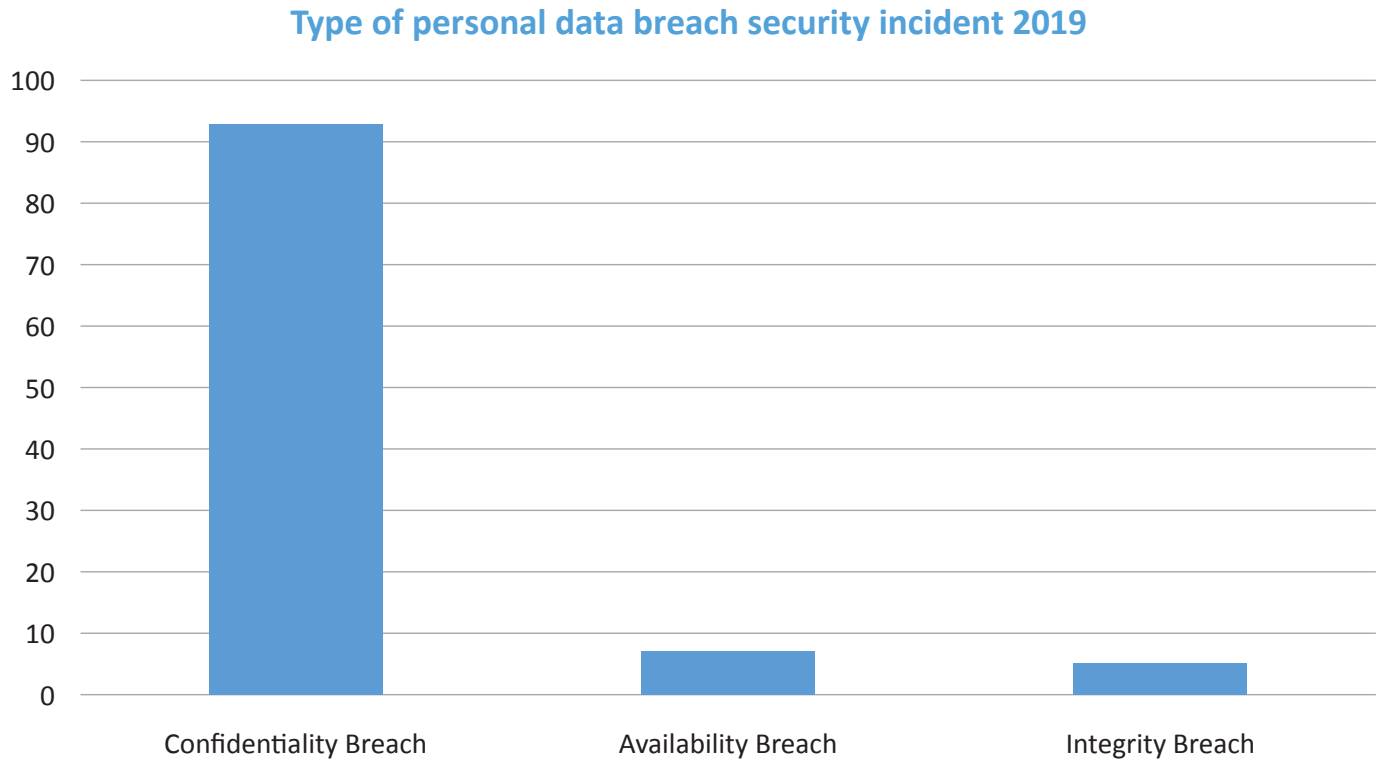


Figure 4. Security incident types of data breach notifications received by the EDPS in 2019

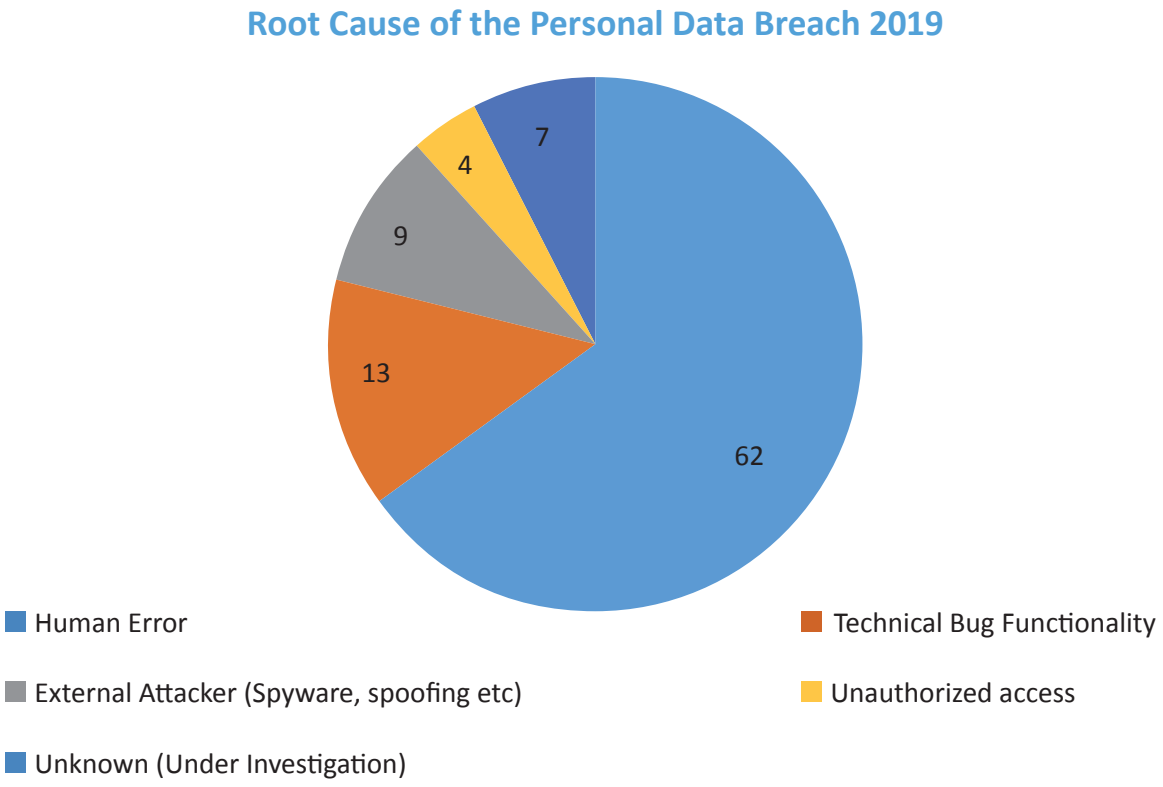


Figure 5. Root cause of personal data breach incidents received by the EDPS in 2019

3.2.4 Cooperating with national DPAs

Each EU Member State has at least one independent data protection authority (DPA). They are 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.

EU 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 EU.

Data Protection in Practice: the European Data Protection Case Handling Workshop

At the end of November 2019, the EDPS hosted the 31st edition of the annual European Data Protection Case Handling Workshop, where we welcomed colleagues from 28 EU and non-EU data protection authorities.

The unique set-up of the workshop provides an opportunity to meet a wide array of practitioners and to share our experiences of investigating complaints, providing guidance to controllers and enforcing data protection law. It is a platform to exchange with colleagues from our sister DPAs at national level about our supervisory and enforcement tasks.

Assistant Supervisor Wojciech Wiewiórowski opened the workshop while a number of larger and smaller DPAs, including the EDPS, also took to the stage during the workshop, to kick-start discussions on various aspects of supervising and enforcing the

@EU_EDPS

Data Protection in Practice: The European Data Protection Case Handling Workshop was an opportunity to meet a wide array of practitioners & to share experiences on providing guidance, investigating complaints & enforcement. Read blogpost by @W_Wiewiorowski https://europa.eu/!rB68kR

General Data Protection Regulation (GDPR), Regulation 2018/1725 and other pertinent (national) legislation, as well as presenting practical case studies that guided our conversations. Among the topics discussed were prior consultations, data brokers and credit reference systems, cross-border case handling, investigative practices and the determination of corrective measures.

Through our participation in events like these, the EDPS underlines our support for a strong regulatory framework and continues to push for the solid implementation of this framework in practice.

The Hague Forum: seeking solutions for cloud contracting

When using the products and services of IT service providers, EU institutions outsource the processing of large amounts of personal data. Nevertheless, like all controllers operating within the European Economic Area (EEA), they remain accountable for any processing activities carried out on their behalf. They must assess the risks, and have appropriate contractual and technical safeguards in place to mitigate those risks.

It was with this in mind that, in April 2019, the EDPS launched an investigation into the use of Microsoft products and services by EU institutions. It assessed whether the contractual agreements between Microsoft and the EU institutions comply fully with data protection rules and whether appropriate measures are in place to mitigate risks to the data protection rights of individuals when the EU institutions use Microsoft products and services.

The preliminary results of the investigation revealed serious concerns. Similar risk assessments, carried out by the Dutch Ministry of Justice and Security, confirmed that public authorities in the Member States faced comparable issues. In search of a solution for all public authority users of Microsoft products and services, we joined forces to organise the first EU software and cloud suppliers customer council in The Hague, on 29 August 2019.

Over one hundred representatives from public institutions all over Europe attended this first meeting, where we established The Hague Forum. The Forum will act as a platform for discussion about two subjects:

1. how to take back control over the IT services and products offered by the big IT service providers;

2. the need to collectively create standard contracts instead of accepting the terms and conditions as they are written by these providers.

Collectively, we are stronger and wield more influence. Achieving our aims is therefore more likely.

A second meeting of the Hague Forum will take place in March 2020.

Processing patients' data: EDPS and EDPB issue first Joint Opinion

Under the new rules on data protection for EU institutions and bodies, the European Commission may, in certain cases, request a Joint Opinion on a legislative proposal or a draft implementing measure from the EDPS and the European Data Protection Board (EDPB).

The first request for such an Opinion came on 13 May 2019, and concerned the data protection aspects of the draft Implementing Decision providing for the establishment, management and functioning of the eHealth network, and repealing Commission Implementing Decision 2011/890/EU.

The eHealth Network is a voluntary network of authorities responsible for eHealth, representing each Member State. It was established under European Commission Implementing Decision 2011/890/EU, which also sets out the rules for the management and functioning of the network.

One of the main objectives of the eHealth network is to improve the interoperability of national digital health systems, making it easier to exchange patient data found in ePrescriptions, Patient Summaries and electronic health records. To facilitate this interoperability, the eHealth network and the Commission developed the eHealth Digital Service Infrastructure (eHDSI), an IT tool that enables the exchange of health data under the Commission's Connecting Europe Facility programme.

Our Joint Opinion addressed the processing of patient data in the eHealth Digital Service Infrastructure and, in particular, the Commission's role in this. The EDPS and

the EDPB confirmed the European Commission's assessment of its role as a processor within the eHDSI, in the situation covered by the Implementing Decision, and specifically for the processing of patients' data within the eHDSI, while also confirming that the Member States should indeed be considered joint controllers. We also reminded the Commission of the need to clearly set out all of its duties as a processor in this processing operation in the proposed Implementing Act, as required by the data protection rules for EU institutions.

3.2.5 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 four investigations into EU institutions' compliance with data protection rules. These concerned contractual agreements between the EU institutions and Microsoft (see section 3.2.4), the European Parliament's election website, Wi-Fi in the European Parliament and EU institutions' use of photo booths.

Communicating about the EU 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 therefore seemed necessary for the EDPS to investigate this processing operation, in order to make sure that the Parliament collected and used personal data in a transparent and lawful way. As a result, 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, and when they failed to do this before our deadline, we issued a second reprimand.

In November 2019, once the Parliament had finished informing individuals of their revised intention to retain personal data collected by the website until 2024, we visited the Parliament to check their data retention processes. During the visit, we confirmed that the data of those users who had not accepted the updated privacy policy had been deleted and checked the functioning of data retention procedures.

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.

Wi-Fi in the European Parliament

In October 2019, an article appeared in the press concerning the European Parliament's Wi-Fi network. It reported that the European Parliament reserves the right to monitor individual users of its Wi-Fi network, including journalists and other visitors, who log in to the Parliament's public Wi-Fi network.

Following the press report, the EDPS launched an inquiry into the Parliament's processing of personal data relating to the users of its Wi-Fi network. This investigation is ongoing. We also received complaints on the matter from the International Press Association and a European Parliament staff member.

While the primary focus of our investigation is on ensuring that the Parliament's Wi-Fi system is

compliant with the rules set out in Regulation 2018/1725, we also aim to assess the compliance of Wi-Fi systems in the other EU institutions and bodies and raise awareness of the requirements set out in the Regulation.

The use of photo booths by EU institutions

In October 2019 we launched an investigation into the use of photo booths, focused initially on their use by the European Parliament, the European Commission, the Council and the European Economic and Social Committee (EESC).

EU institutions often use photo booths as an activity during the annual EU Open Day (see section 6.1.2), to reach out and raise awareness of EU activities among the public. As one of the main aims of the Open Day is to enhance the EU's reputation, it is in the interest of the institutions to ensure that photo booths, and all other activities, are set up in a way that ensures the protection of the personal data of those who use them.

We requested specific information from the EU institutions mentioned above, as well as OLAF, on their use of photo booths and are now in the process of examining their replies. Once our assessment is complete, we plan to issue guidance on how to use photo booths in compliance with Regulation 2018/1725. This will ensure that the institutions are able to continue using photo booths, but in a more data protection-friendly manner.

3.2.6 Exercising our powers

Regulation 2018/1725 grants the EDPS certain powers, which we can use to ensure that the EU institutions comply with their data protection obligations. One of these powers is to introduce a ban on specific types of data processing.

On 30 September 2019, we issued a temporary ban on the production of social media monitoring (SMM) reports by the European Asylum Support Office (EASO). EASO was using the SMM reports to give management and relevant stakeholders news on the latest shifts in asylum and migration routes and smuggling offers, as well as an overview of conversations in the social media community relating to key issues, such as flight, human trafficking and other asylum systems and processes. EASO was doing this without the necessary legal basis required to do so.

Social media monitoring tools in general raise a number of serious data protection concerns. In EASO's case, these included a *chilling effect* - the tendency for users to self-censor their online content if they think it might be monitored -, the high risks posed to the fundamental rights of the individuals and groups monitored, the lack of fairness and transparency involved in processing this data and the vast number of social media users implicated. Given these concerns, EU institutions, bodies and agencies must not only have a specific legal basis for carrying out social media monitoring, which EASO does not currently have, but also complement such processing operations with robust additional safeguards.

We verified that the ban had been implemented when we visited EASO in November 2019.

3.2.7 Protecting privacy in the EU institutions

There are several ways in which the EDPS is able to ensure the protection of privacy in the EU institutions. These include investigating complaints submitted against EU institutions, providing advice to EU institutions on planned data processing operations and providing general advice through the publication of Guidelines.

The EDPS provides advice to EU institutions on specific (planned) processing operations and any other question related to data protection (Article 57(1)(g)). Depending on the needs of the consulting EU institution and the complexity of the case, our advice can take different forms – from calls to our DPO hotline, to informal advice at staff level, to formal letters signed by the Supervisor.

These consultations help the EU institution, by providing advice on how to apply the Regulation, but they also help the EDPS, by providing an overview of recurrent issues. In line with the principle of accountability, consulting the EDPS does not mean that we will do the controller's work for them. We point EU institutions in the right direction and give recommendations, but final responsibility for the processing activity remains with the controller.

In some cases, the Regulation obliges EU institutions to consult the EDPS on planned processing operations or documents governing them and, in certain circumstances, to obtain

data protection impact assessment (Article 40) and consultations on *internal rules for restricting data subjects' rights* (Article 41(2)) are mandatory. Ad-hoc contractual clauses and provisions in administrative arrangements for adducing appropriate safeguards for extra-EU transfers of personal data *require prior authorisation* (Article 48(3)).

In our replies to such consultations and authorisation requests, we provide input on any necessary improvements.

Ensuring access to personal data

We received a complaint from a member of staff at an EU institution. He wanted access to his personal data relating to a harassment complaint, submitted against him by a colleague, which had been declared inadmissible.

The EU institution claimed that giving him access to this data would undermine the alleged victim's rights and freedoms. They also maintained that, as no disciplinary procedure had been initiated against him, his right to defend himself could not outweigh the need to ensure the confidentiality of the procedure. As the harassment allegations also targeted two other members of staff, against which a procedure had been initiated, the complainant was informed that his right of access to his data would be reconsidered once the procedure was concluded.

The EU institution informed us that they were obliged to restrict the complainant's right of access to the data for two main reasons:

- the harassment allegation against the complainant and the two other individuals was submitted in the same document;
- there was a need to ensure the confidentiality of the alleged victim of harassment and of the witnesses, in order to protect them from any possible retaliation.

The right of access to personal data is a continuous and permanent right, unless a necessary restriction is applicable. In this case, we found no such necessary restriction. The complainant's factual and legal situation changed once the claim against him was declared inadmissible, and the EU institution should therefore have re-examined whether the refusal of access was truly justified.

The EU institution should have applied the principle of data minimisation and provided the complainant with the relevant and necessary information relating to his specific request. That the facts of the harassment complaint submitted against the other two members of staff were closely related to those of the complainant was not grounds for linking the ongoing procedure against them to the complainant or his personal data.

In addition, the argument that the complainant did not need to defend himself contradicted the institution's reasoning for applying the restriction on access to his personal data in the first place: that there was an ongoing procedure, and they must protect the rights and freedoms of those involved.

Finally, since the harassment complaint against the complainant was declared inadmissible, the EU institution should have performed an objective assessment to evaluate the likelihood and severity of the risks that processing the complainant's data might pose to his rights and freedoms, balancing these against the rights and freedoms of the alleged victim.

We requested that the EU institution take all reasonable steps to ensure that the complainant's right of access to his personal data was granted.

Protecting the privacy of the press

As part of the online registration process for an event organised in an EU Member State by one of the European Parliament's political groups, members of the press were required to upload their press credentials. Among other information, these credentials list each journalist's home address.

We investigated a complaint relating to this process, and issued a Decision on 19 February 2019, concluding that this processing operation was in breach of the

applicable data protection rules. This is because the collection of the home addresses of journalists in this case was neither lawful, as it was not necessary for the organisation of the conference, nor did it meet the requirements for data quality, specifically the obligation to not collect excessive amounts of data.

The organisers of the event claimed that some of the participants in the event had received threats of violence in the past, necessitating the collection of information such as home addresses from journalists. We, however, judged that the unnecessary collection of this information would likely have created increased security risks, which could also have involved third parties, such as the family members of journalists.

Given the vital role of journalism in democratic discourse, the creation of such unnecessary risks in performing their job might have a negative impact on their freedom of expression. We therefore informed the political group that they should refrain from collecting such data in future and that any future incidents of unlawful processing of personal data may result in EDPS corrective action, including a fine.

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

In 2019, the EDPS received 210 complaints, a decrease of 30% compared to 2018. Of these, 151 were inadmissible, the majority relating to data processing at national level as opposed to processing by an EU institution or body. We replied to all inadmissible complaints, directing the complainant to the relevant authority.

The remaining 59 complaints required in-depth inquiry, a comparable number to the statistics from 2018.

In 2019, we issued 48 complaint decisions on admissible complaints.

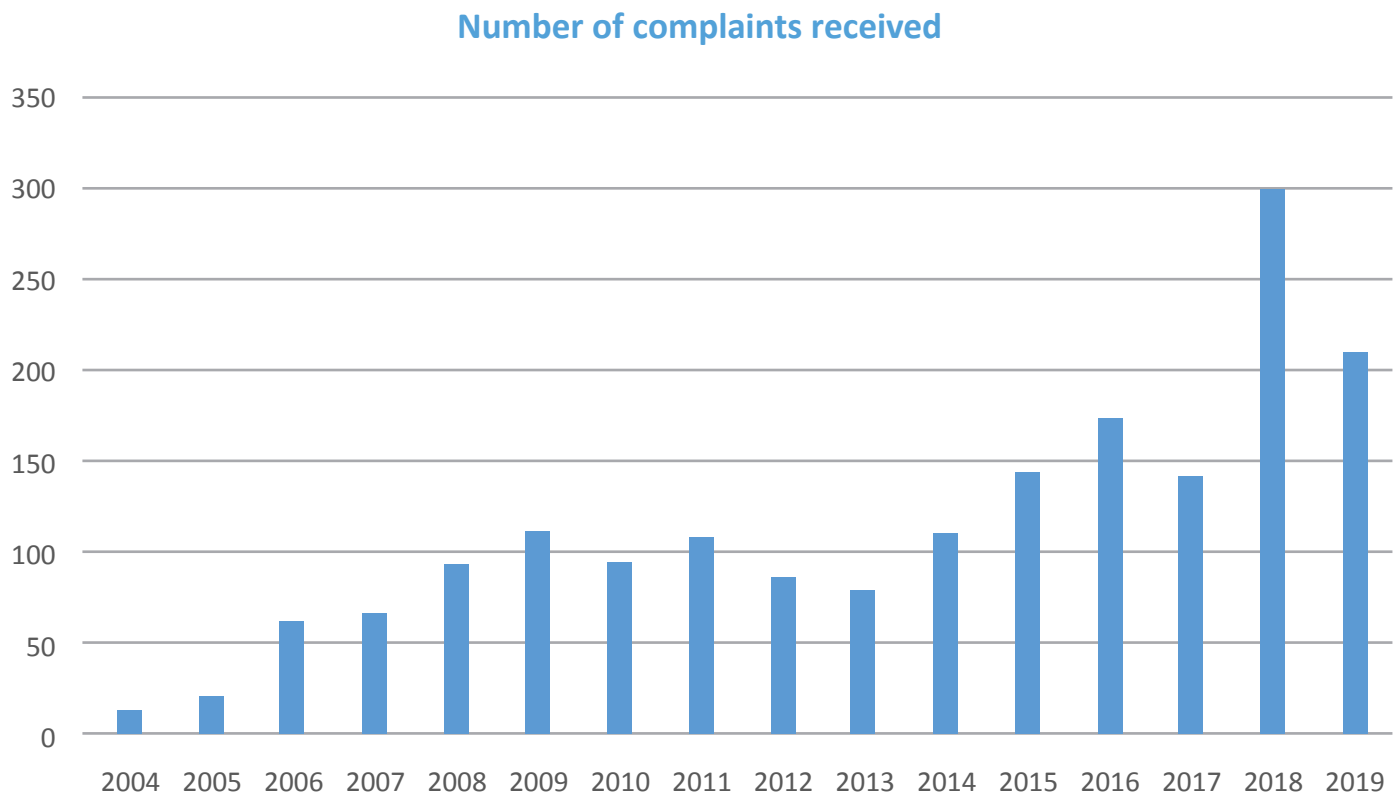


Figure 6. Evolution of the number of complaints, including inadmissible complaints, received by the EDPS

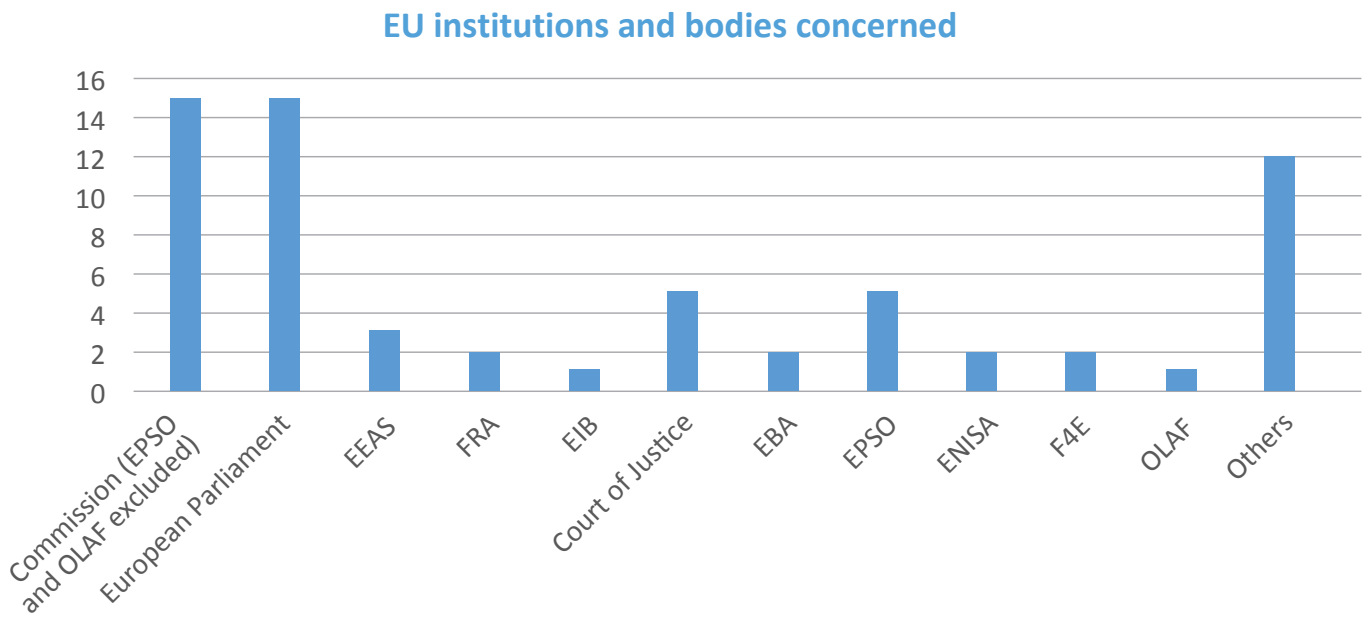


Figure 7. EU institutions and bodies concerned by complaints received by the EDPS in 2019

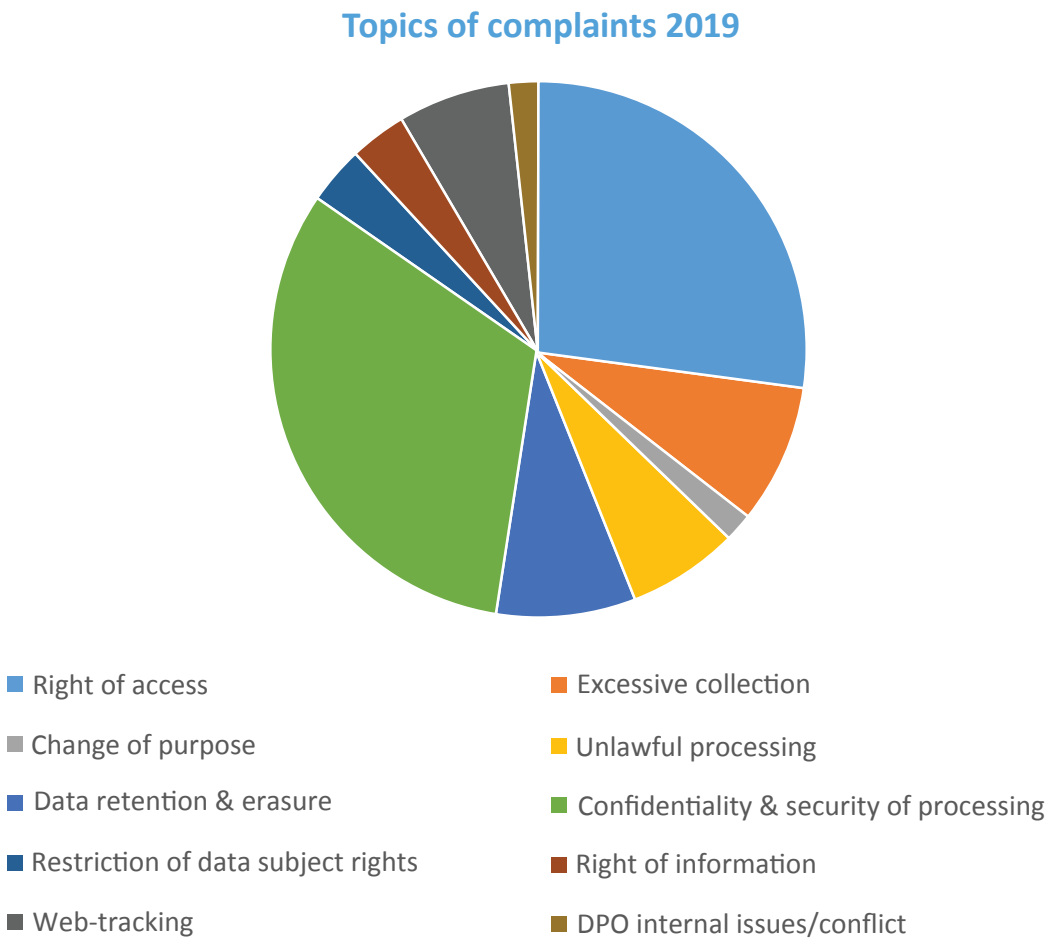


Figure 8. Type of violation alleged in complaints received by the EDPS in 2019

Making privacy-friendly policy easier

On 19 December 2019, we published Guidelines on assessing proportionality. These aim to provide policymakers with practical tools to help assess the compliance of EU proposals that would have an impact on the fundamental rights to privacy and the protection of personal data with the Charter of Fundamental Rights.

The General Data Protection Regulation (GDPR) is built on Article 8 of the EU Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the European Union, which state that all individuals have the right to the protection of their personal data. The EU legislator must therefore make sure that all EU legislation complies with these overarching constitutional principles. In addition, any restriction of these rights must comply with certain criteria:

- it must be provided for by law;
- it must respect the essence of the fundamental rights in question;
- it must be both necessary and proportional, taking into account not only the aims of the measure itself, but also the need to protect rights and freedoms in general.

As new EU proposals now routinely imply the processing of personal data, it is vitally important to ensure that policymakers are well-equipped to adequately assess the necessity and proportionality of a proposed measure. Building on relevant case law from the Court of Justice of the European Union and recent EDPS legislative Opinions and formal Comments, the EDPS Proportionality Guidelines, combined with our Necessity Toolkit, provide practical guidance to help address these key dimensions from the start of the legislative process, therefore facilitating responsible and informed EU policymaking.

As the new Commission gets to work, we are certain that both our Proportionality Guidelines and the Necessity Toolkit can play a significant role in simplifying the challenges faced by policymakers, and therefore help them to ensure that fundamental rights are always adequately protected.

The concepts of controller, processor and joint controllership

The roles and concepts of controller, processor and joint controllership are not new. However, the GDPR and the equivalent rules for the EU institutions set out in Regulation 2018/1725 introduced some changes, which have led to some questions about these concepts, and the respective roles and responsibilities assigned to each in particular.

Recognising a need for guidance on this issue, on 7 November 2019 we published our Guidelines on the concepts of controller, processor and joint controllership under the data protection rules for the EU institutions set out in Regulation 2018/1725.

Aimed primarily at those working in the EU institutions, but also useful for others, the Guidelines provide practical advice and instructions on how to comply with Regulation 2018/1725 by clarifying the concepts of controller, processor and joint controllership, based on the definitions provided in the Regulation. The Guidelines also explain the distribution of obligations

@EU_EDPS

Assessing the #Proportionality of measures that limit the fundamental rights to #privacy and #protection of personal data - #EDPS launched a stakeholders' consultation on the draft Guidelines. Read more https://europa.eu/!nC64Hp

@EU_EDPS

Concepts of controller, processor & joint controllership refer to different roles of entities carrying out specific processing operations. #EDPS Guidelines help #EUI identify their role, responsibilities & steps to ensure best data protection practice https://europa.eu/!ny44Vr

and responsibilities between these roles, particularly in cases where data subjects decide to exercise their rights.

To help put this into practice, the Guidelines include specific case studies, checklists and charts on controller-processor, separate controllership and joint controllership situations. We hope they prove a useful tool in ensuring the protection of personal data in the EU institutions and beyond.

3.2.8 Catching up with the EU institutions

Audits and visits are two tools we can use 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 among those who work for the EU institutions.

Audits and visits

We carried out nine audits and two compliance visits in 2019, at a variety of different EU institutions and bodies. Audits are used to assess how well an EU institution is implementing data protection rules, while during compliance visits we work with an EU institution to draw up a roadmap to ensure that they implement the rules. We share the results of our audits with the institutions concerned and follow up with each institution after both audits and compliance visits, to ensure that they have implemented our recommendations.

Under Regulation 2018/1725, the focus of our audits and visits has shifted slightly, with a greater emphasis now on ensuring that the EU institutions adopt 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.

Remote inspections of EU institutions' websites

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.

As the number of web services reported by the institutions totals more than 1300, 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, which we announced in June 2019, revealed that several of the websites inspected were not compliant with Regulation 2018/1725, nor with the applicable provisions of the ePrivacy Directive, and did not follow the EDPS 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 insufficient connection security.

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.

The Website Evidence Collector

To carry out inspections of EU institution websites, we developed a number of specialised software tools. This included our Website Evidence Collector (WEC), 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).

Following the results of the first wave of our website inspections, we published the WEC on the EDPS website and on the code collaboration platform GitHub. It is now available as free software under the EU public license (EUPL), meaning that anyone can download and use it on 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. By sharing the WEC, we hope to provide DPAs, privacy professionals, data controllers and web developers with the tools to carry out their own website inspections.

Our work on the WEC, and our efforts to make it available to others, achieved international recognition, earning the Global Privacy and Data Protection Award for innovation. We received the award at the annual International Conference of Data Protection and Privacy Commissioners (ICDPPC), which took place in October 2019 in Tirana, Albania. Since then, an increasing number of DPAs and companies have made use of the tool.

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 carry out remote inspections of mobile apps in addition to websites.

@EU_EDPS

#EDPS Website Evidence Collector receives Global #Privacy & #DataProtection Award for innovation at #ICDPPC2019! @W_Wiewiorowski The award emphasises that DPAs can approach enforcement tasks in technically sophisticated way to address new DP challenges europa.eu/!ph37BY

3.2.9 Developing and sharing technological expertise

Technological expertise is now essential if we are to ensure effective data protection. The digital revolution has compelled DPAs and other regulators to develop skills in this area. This task is also now part of their job description, as both the GDPR and the equivalent rules for the EU institutions require DPAs to monitor the impact of new technologies on the protection of personal data.

The EDPS has consistently aimed to lead this trend, by sharing helpful analyses of new technological developments.

Smart glasses

One example of our efforts to share information on new technologies is our Technology Monitoring Brief on smart glasses and data protection, published in January 2019.

Though smart glasses may seem like something from a science fiction film, they are in fact increasingly available and increasingly used, whether by public authorities, businesses or individuals. The interest in this technology shown by law enforcement authorities around the globe indicates its potential.

However, while smart glasses may prove useful in a variety of contexts, including technical maintenance, education and construction, they can also have serious implications for privacy, especially when the process used to develop them does not take privacy by design into account.

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, as well as assessing possible future developments.

TechDispatch

Our TechDispatch publication is another way in which we hope to contribute to the ongoing discussion on new technologies and data protection. Launched in July 2019, each issue explains 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, as well as links to further reading on the topic.

We published three issues of TechDispatch in 2019. These addressed Smart Speakers and Virtual Assistants, Smart Meters in Smart Homes and Connected Cars. More issues, addressing a variety of new technologies, are planned for 2020 and beyond.

With work on EDPB Guidelines on voice assistants now underway, we hope that our analyses of new technologies will continue to contribute to ongoing discussions and inspire new debates.

Blockchain

Given the complexity of applying blockchain technology in privacy-friendly ways, EU DPAs have been cautious about expressing their opinion on this and related technologies. This will change in 2020, however, with the EDPB set to issue guidance on the topic.

Blockchain technology is currently used as an enabler for Bitcoin and other *crypto-currencies*. It is the most successful implemention so far of Distributed Ledger Technology (DLT), which provides for databases with many replicas under the shared control of distinct, often autonomous participants.

International humanitarian organisations have considered using Blockchain technology for the distribution of goods and services. However, much care is necessary to ensure that strong data protection safeguards are in place when dealing with the personal data of vulnerable people such as refugees and children. These organisations have therefore been looking to improve their understanding of the opportunities and risks related to privacy when using blockchain.

Throughout 2019, the International Committee of the Red Cross organised a series of workshops to update their Handbook on Data Protection in Humanitarian Action, with the aim of providing specific data protection guidance on blockchain. We participated in these debates in our role as a member of both the EDPB and the Advisory Board set up for the workshop series on Data Protection in Humanitarian Actions.

A workshop on blockchain held in February 2019 in Geneva, for example, brought together humanitarian organisations such as the Red Cross, UNHCR, and Médecins Sans Frontières, alongside technology experts from academia and European DPAs. The results of this discussion will feed into the next edition of the Handbook, which will be published in 2020.

3.2.10 The Internet Privacy Engineering Network (IPEN)

Launched in 2014, the Internet Privacy Engineering Network (IPEN) brings together experts from a range of different areas to encourage the development of engineering solutions to privacy problems. Through facilitating exchange between regulators, researchers and developers that build privacy into new and existing digital tools, the Network aims to promote and advance state-of-the-art practices in privacy engineering.

We organised two IPEN events in 2019. The first of these was a special Data Protection Day IPEN workshop in Brussels, which took place on 28 January 2019. The workshop was organised as a side event at the 2019 CPDP conference, and brought together over 70 privacy experts and engineers from public authorities, industry, academia and civil society. Our main objective was to determine what privacy engineering methodologies and best practices already existed, and to figure out the necessary steps for them to become shareable, useable tools that can support

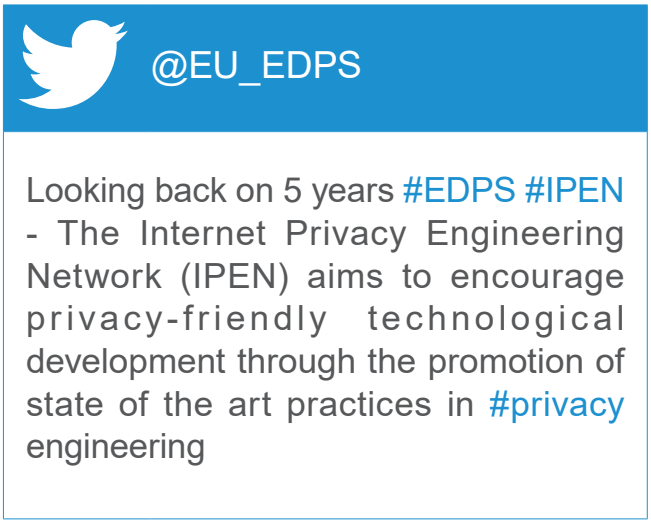
organisations and developers in integrating data protection requirements across the world.

The workshop was also an opportunity to discuss the relationship between state-of-the-art technologies and privacy and data protection. Legal obligations under the new EU data protection framework require controllers to consider the state of the art not only in data processing security, but also when ensuring data protection by design and by default. While there are guidelines defining the state of the art in IT security, there is less operational guidance on what state of the art is in data protection by design. Those involved in the technical and legal processes, therefore, do not necessarily have a shared understanding of what data protection by design means in practice.

The discussion inspired a more targeted approach to our annual IPEN workshop, which took place on 12 June 2019, in Rome, and focused on how to identify state of the art in data protection by design in a concrete sense, including specific fields of application. When putting data protection by design into practice, controllers and developers, regulators and legal experts all need to understand what they should – and should not – consider as state of the art technology.

The workshop explored four key areas: the concept of state of the art in relevant fields; the consideration of business models enabling individuals to be in control of their data; privacy engineering and pseudonymisation and anonymisation.

After another successful session, the EDPS looks forward to engaging with IPEN in future events to ensure a stronger, collaborative and effective approach to privacy engineering.



3.2.11 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.

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.

Supervising data processing activities in the field of law enforcement presents a number of challenges. Individuals' rights are often restricted and the impact of data processing activities on their rights and freedoms is significant, especially as many of those concerned are in particularly vulnerable situations. The data processing activities used are often opaque to individuals, which makes it difficult for them to know who is processing their data and for what purposes, while the many crime areas in which Europol is active place different imperatives and constraints on Europol's work. In addition to this, the complex IT systems used to process the large volume of personal data Europol deals with makes the task of ensuring data protection compliance even more difficult.

It is important that the EDPS engages in a constructive dialogue with Europol, aimed at ensuring that data protection, privacy and other fundamental rights recognised in the EU Charter are adequately protected.

The results of this dialogue often have an impact across the wider law enforcement community. The very nature of Europol means that it performs its tasks in constant interaction with the competent authorities of the Member States, as well as with its partners across the globe. This means that any data protection regime implemented at Europol has a more widespread impact that we must take into account when carrying out our supervisory activities.

Cooperation with Europol

We work closely with Europol's Data Protection Function (DPF) team and other operational staff, providing them with informal advice when needed, notably through bi-monthly meetings. This helps us to anticipate consultations and other issues relating to data processing and to define and plan for future activities, such as inspections or inquiries. In 2019, the EDPS and the DPF met seven times in either The

Hague or Brussels, on 17 January, 22 March, 14 May, 5 July, 30 August, 14 October and 4 December 2019.

Cooperation at management level is equally important and meetings between the EDPS and Europol higher management take place periodically. On 1 April 2019, Catherine De Bolle, Executive Director of Europol, met with EDPS Giovanni Buttarelli in Brussels. The Executive Director also met with Assistant EDPS Wojciech Wiewiórowski on the margins of the Joint Parliamentary Scrutiny Group of Europol meetings in February and September 2019.

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 we therefore need to be 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 that originate in the Member States. The EDPS provides the secretariat for this Board, which meets at least twice a year.

In 2019, meetings of the Cooperation Board took place on 8 May and 28 November 2019. We used them as an opportunity to share information on our supervisory activities, including the main findings of our inspections, focusing on issues relevant to both Europol activities and practices at national level. These included the increasing number of large datasets sent to Europol by Member States, the processing of data on suspects who are under 18 years of age and the consequences of Brexit. A particular focus for discussions was FIU.net (see *Exercise of Powers*), a decentralised information network operated by Europol, which supports the national Financial Intelligence Units (FIUs) in their fight against money laundering and the financing of terrorism.

In addition to our work through the Cooperation Board, we cooperate with representatives from the DPAs to carry out inspections (see *Inspections and Inquiries*).

We are also required to report to the Joint Parliamentary Scrutiny Group (JPSG), which is responsible for holding Europol politically accountable for its activities, at least once a year, to discuss Europol's compliance with the rules and principles relating to the protection of personal data. In 2019, two meetings of the JPSG took place and the EDPS was invited to attend both, in Bucharest on 25 February 2019 and in Brussels on 23 September 2019.

Supervisory activities

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

Operational analysis projects

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.

In 2019, Europol informed us about the creation of a new OAP aimed at supporting investigations into administrators and moderators of websites and forums facilitating crime on the Dark Web. All ongoing analysis projects are listed and described on the Europol website.

Opinions

We provide advice on all matters concerning the processing of personal data at Europol, in the form of Opinions. This might be on our own initiative or in response to a consultation.

For any new data processing activity that involves the processing of sensitive data or that might pose a specific risk to an individual, Europol must notify the EDPS. This notification must include a general description of the planned processing operations, an assessment of the risks posed to the freedoms of individuals and a comprehensive list of the measures envisaged to address those risks. We examine their proposals and provide recommendations.

In 2019, we issued three Opinions following prior consultations. The Opinions concerned the following tools:

- **SIENA 4.0:** the updated version of Europol's secure message exchange system. It is used to manage the exchange of operational and strategic crime-related information between Europol, Member States and Europol's other partners.
- **Cryptocurrency portal:** a platform that Europol intends to create, which will help law enforcement authorities to query cryptocurrency systems and to monitor activities at particular addresses.
- **Access to PNR:** Europol developed a procedure to request Passenger Name Record (PNR) information from specialised units in Member States, known as Passenger Information Units (PIUs), in compliance with the PNR Directive. PNR data is information provided by passengers when they book tickets and check in for flights, as well as data collected by air carriers for their own commercial purposes.

Inspections and inquiries

General and thematic inspections are an important part of our supervisory activities. In each inspection, we carefully audit selected legal and technical aspects of data processing and check that data security complies with international standards.

The 2019 annual inspection took place from 3-6 June 2019 and focused on the processing of data in the area of terrorist financing, as well as the fight against money laundering and illegal activities on the Dark Web. We also checked Europol's use of derogations to transfer personal data to non-EU countries. Subject to strict requirements, such transfers are permitted in exceptional circumstances, such as to support investigations in the aftermath of a terrorist attack or to prevent an immediate and serious threat to public security.

Another area for inspection concerned the emerging trend for Member States to send increasingly large datasets to Europol, due to the collection of larger amounts of personal data relating to criminal investigations and criminal intelligence operations at national level. We also verified Europol's encryption methods, as well as the implementation of selected recommendations from our previous inspection reports.

As for previous inspections, we invited 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 and how these can be addressed. For the 2019 inspection, three experts from the DPAs of Germany, Greece and Italy joined the EDPS team.

The inspection resulted in a number of recommendations for improvement, which we outlined in an inspection report sent on 6 December 2019 to the Executive Director of Europol and shared with the Cooperation Board. The recommendations aim to initiate activities that will not only improve data protection but also the efficiency of Europol's operational activities. We will follow up on their implementation closely.

On 5-6 February 2019, we also carried out a targeted inspection. This focused on the verification role played by Europol in the implementation of the Terrorist Financing Tracking Programme (TFTP) Agreement between the EU and the US. The Agreement relates to the exchange of financial information between the EU and the US to construct financial intelligence, which is used to help tackle terrorism.

Europol's role in the TFTP process is to assess whether the data on financial transfers stored on EU territory and requested by the US authorities is necessary for the fight against terrorism and against the financing of terrorism. Europol also makes sure that each request is tailored as narrowly as possible, in order to minimise the amount of data transferred to the US. Europol is only responsible for verifying the requests, it does not have access to any data subsequently transferred to the US.

Our inspection found that, in general, Europol does a good job of verifying US requests. However, we also made eight recommendations for Europol to consider when carrying out these activities. Most importantly, the EDPS recommended that Europol ask for additional information from the US authorities in order to be able to check that their requests actually meet necessity requirements in terms of countries and message types.

Other recommendations concerned both the verification process and security measures, with the aim of ensuring that the methods used by Europol contribute to keeping the EU safe and secure without unduly compromising the fundamental rights to data protection and privacy. The public version of the report can be found on the EDPS website.

In addition to inspections, we are also able to conduct own initiative inquiries on issues that come to our

attention in the course of our other supervisory activities.

Complaints

We deal with any complaints from individuals that relate to the processing of their personal data by Europol.

Of the three complaints received in 2019, only one of them was admissible and concerned a request for access to data. Europol replied to the request by saying that they had not processed any data relating to the individual in question, who then challenged Europol's reply before the EDPS. We examined the complaint and carried out the necessary checks, including on the-spot verification at Europol's premises. Following this examination, the EDPS confirmed Europol's findings.

Data breaches

Europol is required to inform us, without undue delay, of any personal data breach that occurs at Europol. 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 to inform them if it is considered significant. We continually monitor Europol's internal procedure for dealing with such cases as part of our bi-monthly meetings and provide our input.

Exercise of powers

On 19 December 2019, we imposed a ban on processing operations carried out by Europol in the technical operation of FIU.net. We found these processing operations to have breached the provisions governing the processing of personal data.

FIU.net is a decentralised information network designed to support national Financial Intelligence Units (FIUs) in their fight against money laundering and the financing of terrorism. It can be used for for the exchange of data on individuals involved in suspicious monetary transactions.

At issue was the question of whether Europol could act as the technical administrator of this network, considering the restrictions outlined in the Europol Regulation on the categories of individuals about whom Europol can process personal data. To comply with the rules, individuals involved in suspicious transactions would have to be considered as *suspects*. FIUs, however, act before the start of any criminal proceeding or investigation has begun.

As the definition of what constitutes a suspect in the Europol Regulation refers to national laws, we referred the matter to the Europol Cooperation Board. In the Board's advisory opinion of 11 September 2019, it concluded that there was no way to consistently ensure that Europol is legally competent to process all types of information and personal data shared through FIU.net.

Following the opinion of the Cooperation Board, we issued our final decision, stating that the technical administration of FIU.net by Europol was in breach of the Europol Regulation. However, taking into account the importance of FIU.net in the fight against money laundering and terrorism financing at EU level, we suspended the ban until 19 December 2020, in order to allow time for the smooth transition of the technical administration of FIU.net to another entity.

Communication

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

Several EDPS staff members regularly take part in conferences and events dealing with data protection and policing, both as participants and as speakers. Events in 2019 included:

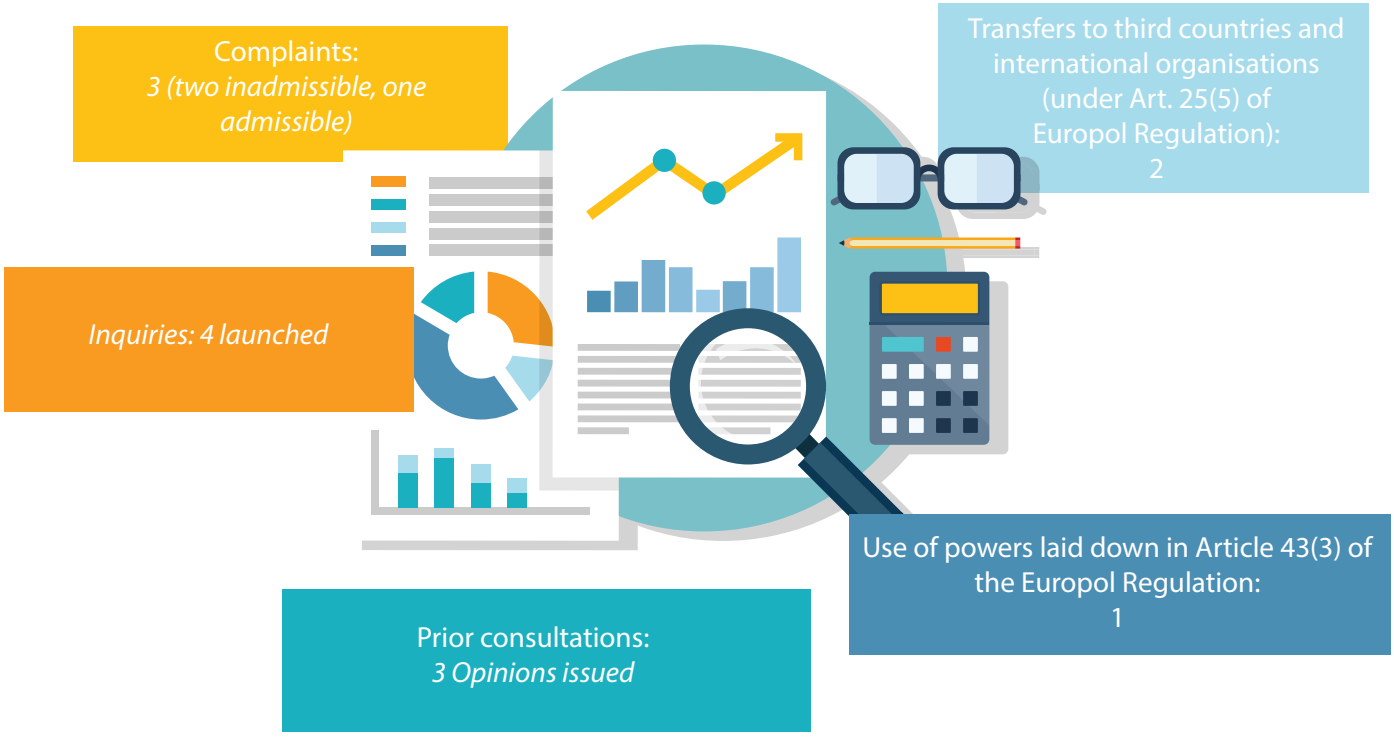
- a panel at the annual Computers Privacy and Data Protection (CPDP) conference on the implementation of the principle of purpose limitation in the Europol Regulation;
- a panel at the annual EDEN Conference on the processing of publicly available information by law enforcement authorities.

Looking to the future

After more than two and a half years in this supervisory position, the EDPS now has strong links with Europol and we have developed a good knowledge of the issues they face when implementing data protection in practice.

However, there are several new challenges that we will face in the coming years that will require specific EDPS scrutiny. These include the emergence of structural data exchanges between justice and home affairs agencies in the EU institutions and between national authorities and EU agencies, as well as the use of new technologies, such as Big Data and Artificial Intelligence.

EDPS Supervision of Europol in 2019:
the statistics



3.2.12 Supervising Eurojust

The EU Agency for Criminal Justice Cooperation (Eurojust) is responsible for supporting and improving coordination and cooperation between the competent judicial authorities in the EU Member States on matters relating to serious organised crime.

On 12 December 2019, a new supervisory framework, known as the Eurojust Regulation, came into force. It appointed the EDPS as the responsible authority for monitoring Eurojust's compliance with the applicable EU rules on data protection. This means ensuring that Eurojust is able to perform its role in judicial cooperation on criminal matters as efficiently as possible, while demonstrating full respect for EU data protection law.

The Eurojust Regulation applies to the processing of personal data for operational activities at Eurojust. It complements the rules set out in Chapter IX of Regulation 2018/1725, which apply to the processing of operational personal data in the EU's law enforcement agencies more generally. The EDPS is also responsible for supervising the processing of personal data for administrative activities at Eurojust, as we do for other EU institutions and bodies, under the rules for data protection in the EU institutions set out in Regulation 2018/1725.

Overseeing data protection compliance at Eurojust includes tasks such as investigating complaints,

conducting inquiries, advising Eurojust on all matters concerning the processing of operational personal data and ensuring that the provisions of the Eurojust Regulation and Regulation 2018/1725 are applied and respected.

The Eurojust Regulation also grants the EDPS certain powers, to ensure that we are able to perform our role effectively. These range from referring a matter to Eurojust in the event of an alleged breach of the rules, to issuing Eurojust with an order to rectify, restrict or erase operational personal data, or even referring the matter to the EU Court of Justice.

This new supervisory task comes two-and-a-half years after taking on responsibility for supervising the processing of operational personal data at Europol, the EU body responsible for cooperating with the law enforcement authorities of the EU Member States to combat serious crime and terrorism. The experience gained through working with Europol has undoubtedly helped to prepare the EDPS for our new role at Eurojust.

Throughout 2019, we worked intensively to ensure that we were ready to take on our new supervisory role at Eurojust. This included working in close cooperation with our colleagues at Eurojust, and with Eurojust's DPO in particular. Regular meetings with Eurojust's DPO have allowed us to gain a better understanding of how Eurojust operates and to ensure that Eurojust understands what is involved in EDPS supervision. We have also given several presentations and organised training sessions for Eurojust staff members.

On 29 October 2019, Assistant EDPS Wojciech Wiewiórowski made an official visit to Eurojust headquarters in The Hague, where he met with the Eurojust President Ladislav Hamran to formalise cooperation.

We have also cooperated closely with Eurojust's previous supervisory authority, the Joint Supervisory Body (JSB) of Eurojust, in order to ensure a smooth transition of supervisory activities to the EDPS. Following a meeting with JSB representatives on 21 November 2019, all JSB supervisory documents, including inspection reports and annual reports, were handed over to the EDPS.

Our first action in our new supervisory role was to issue an Opinion on the Rules of Procedure on the processing and protection of personal data at Eurojust, on 13 December 2019.

@EU_EDPS

#EDPS takes on a new supervisory role at Eurojust - A new supervisory framework for the processing of personal data at the EU Agency for Criminal Justice Cooperation (Eurojust) comes into force today. Read press release europa.eu/!qG87gn

3.2.13 Cooperation with the EFTA Surveillance Authority

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

On 18 December 2019, the EDPS renewed cooperation agreement with ESA. Under this agreement, the EDPS can provide advice to both individuals and ESA itself on the interpretation of ESA's data protection rules, although a final and binding evaluation of this framework remains the remit of the EFTA Court. The agreement will enter into force on 1 January 2020 together with ESA's updated rules on data protection.

We welcomed and supported ESA's move to adopt a new data protection framework applicable to their activities, as it means that individuals should now benefit from the same high standards of protection, whether their data is processed by an EEA Member State, an EU institution or by ESA, ensuring a more coherent approach to personal data protection throughout the EEA.

While the main structure of the data protection framework at ESA is now in place, certain aspects remain to be implemented over the months to come, including updated rules on the role and position of the data protection officer. Under the new cooperation agreement, the EDPS will continue to assist ESA in these tasks.

3.2.14 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.

With this in mind, in 2016 the EDPS launched the Digital Clearinghouse, with the aim of promoting 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.

Held twice a year, the focus of Digital Clearinghouse meetings has gradually evolved and the number of participants has grown. 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.

In 2019, the Digital Clearinghouse met on 5 June and 19 November. During the first of these meetings, authorities addressed the challenges of regulating non-monetary price services. They also discussed big tech companies, with a particular focus on recent consumer decisions and actions taken against Facebook.

The second meeting of the year focused on the regulation of data sharing, analysing the similarities and differences in the approaches of competition, data protection and consumer law to data sharing, and on how to strengthen cooperation in this area.

In a further effort to strengthen cooperation between regulators in the areas of data protection, consumer protection and competition policy, the EDPS also organised an event in collaboration with the Federal Commissioner for Data Protection and Freedom of Information in Germany. The event, which took place on 9 July 2019, took the form of a panel discussion on Data Protection and Competitiveness in the Digital Age. It assessed the intersection between data protection and competition policy in an era in which business models are increasingly reliant on the exploitation of large amounts of personal data.

The next meeting of the Digital Clearinghouse will take place in spring 2020.

3.2.15 Group Privacy

The EDPS is dedicated to ensuring that we remain up-to-date with academic debates in the field of data protection and privacy. Doing so will allow us to better fulfil our role as the data protection authority for the EU institutions and to achieve our objectives as a leading voice on data protection in the international arena.

Engaging with academics working in the field of data protection and privacy is a particularly good way of increasing our knowledge and awareness of current research. On 16 December 2019, we therefore invited Professor Linnet Taylor from Tilburg University to present the concept of *group privacy* to the EDPS. Professor Taylor is one of the editors of the 2017 book *Group Privacy: New Challenges of Data Technologies*.

Group privacy concerns the social, ethical and legal issues posed by group profiling, big data and predictive analysis, all techniques that have been made possible through the development of new technologies. Professor Taylor's presentation helped to highlight some of the key privacy and data protection challenges in this area and provoked a lively debate.

Our efforts to monitor academic trends in the field will continue into 2020 and beyond, in order to ensure that the EDPS remains a centre of excellence for data protection.

3.3 INTERNATIONAL AFFAIRS

Personal data flows freely across borders, but data protection laws remain national or, at best, regional. The EU has therefore adopted a leading role in pushing for greater convergence on data protection at international level, both through encouraging greater international cooperation and through setting the highest standards for data protection globally.

In our Strategy 2015-2019, the EDPS committed to taking a leading position in international discussions, through forging global partnerships. Our principal aim was to contribute to building a global social consensus on the principles relating to data protection. This

involves contributing to discussions on international transfers, as well as strengthening relationships with international organisation and networks.

3.3.1 International data transfers

Schrems II: data transfers between the EU and the US

On 6 October 2015, the EU Court of Justice (CJEU) declared the Safe Harbour Decision regulating data transfers between the EU and the US invalid. Maximilian Schrems, a student from Austria, successfully argued before the Court 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.

Following this success, Schrems brought a new case to court in 2018, now known as *Schrems II*, addressing a number of important questions about the regulation of international data transfers under EU data protection law. Specifically, he questioned the use of Standard Contractual Clauses (SCC) and Safe Harbour's replacement, the Privacy Shield, to transfer data between the EU and the US. The EDPB took part in the hearing before the Court on 9 July 2019 and, as a member of the EDPB, we actively contributed to the preparation of their position.

On 19 December 2019, Advocate General Henrik Saugmandsgaard Øe of the Court of Justice of the EU (CJEU) issued his Opinion on the case. He concluded that Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries remains valid. However, he also stressed that both controllers and supervisory authorities have a responsibility to ensure continued protection. While controllers are expected to conduct a detailed examination of the circumstances surrounding each transfer before using SCCs, DPAs should suspend any data transfers carried out under SCCs in cases where they find there to be a lack of protection.

The Advocate General added that, as the case before the Court concerned the validity of SCCs, it was not the place in which to address issues relating to the Privacy Shield. However, he did express some concerns about the Privacy Shield, relating in particular to US access to personal data and the remedies available to EU citizens in exercising their rights.

We expect the CJEU's final judgement on the case in 2020.

Reviewing the Privacy Shield

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

The third yearly review of the EU-US Privacy Shield took place on 12-13 September 2019. The Privacy Shield Review Team, made up of representatives from the EU's data protection authorities, including the EDPS, took part in the review, which focused primarily on the concerns raised during earlier reviews. Specifically, these related to the commercial aspects of the Privacy Shield and government access to personal data transferred from the EU for law enforcement and national security purposes, including the legal remedies available to EU citizens.

A report on the results was adopted at the November 2019 Plenary meeting of the European Data Protection Board (EDPB). In it, we highlighted our continued concerns relating to lack of oversight in ensuring the compliance of companies with the Privacy Shield principles, particularly in relation to onward transfers of data. Additionally, while we welcomed the appointment of the remaining members of the Privacy and Civil Liberties Oversight Board (PCLOB) and of an Ombudsperson, the way in which personal data is collected and accessed for national security purposes remains problematic.

The Privacy Shield Review Team will present the third annual joint review report to the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament on 9 January 2020.

3.3.2 International cooperation

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.

On 18 May 2018, the Protocol amending the Convention was adopted. It reaffirms the essential principles enshrined in the original Convention text and integrates new safeguards. Known as Convention 108+, the new Modernised Convention 108 was opened for signature on 10 October 2018.

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 (see section 3.1.7). As of March 2018, the EDPS also represents the Global Privacy Assembly (formerly the International Conference of Data Protection and Privacy Commissioners) in the T-PD.

OECD

Up until mid-2019, the EDPS followed the activities of the Organisation for Economic Cooperation and Development (OECD) Working Party on Security and Privacy in the Digital Economy (SPDE). On 1 July 2019, the decision was made to replace the 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 continues to deal with data protection and privacy matters, while the SDE focuses more on cybersecurity and IT issues, such as cryptography. The EDPS follows the activities of both groups.

Since its inception at the beginning of 2019, we have also been involved in the work of the OECD Privacy Guidelines Expert Group (PGEG). We participated in several preparatory conference calls, as well as in two PGEG workshops. The first of these took place in Paris on 6 May 2019 and focused on accountability. The second took place on 18 November 2019, during the first meeting of the DGP, and was dedicated to emerging enforcement challenges, such as Artificial Intelligence, international collaboration and innovative regulatory approaches.

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.

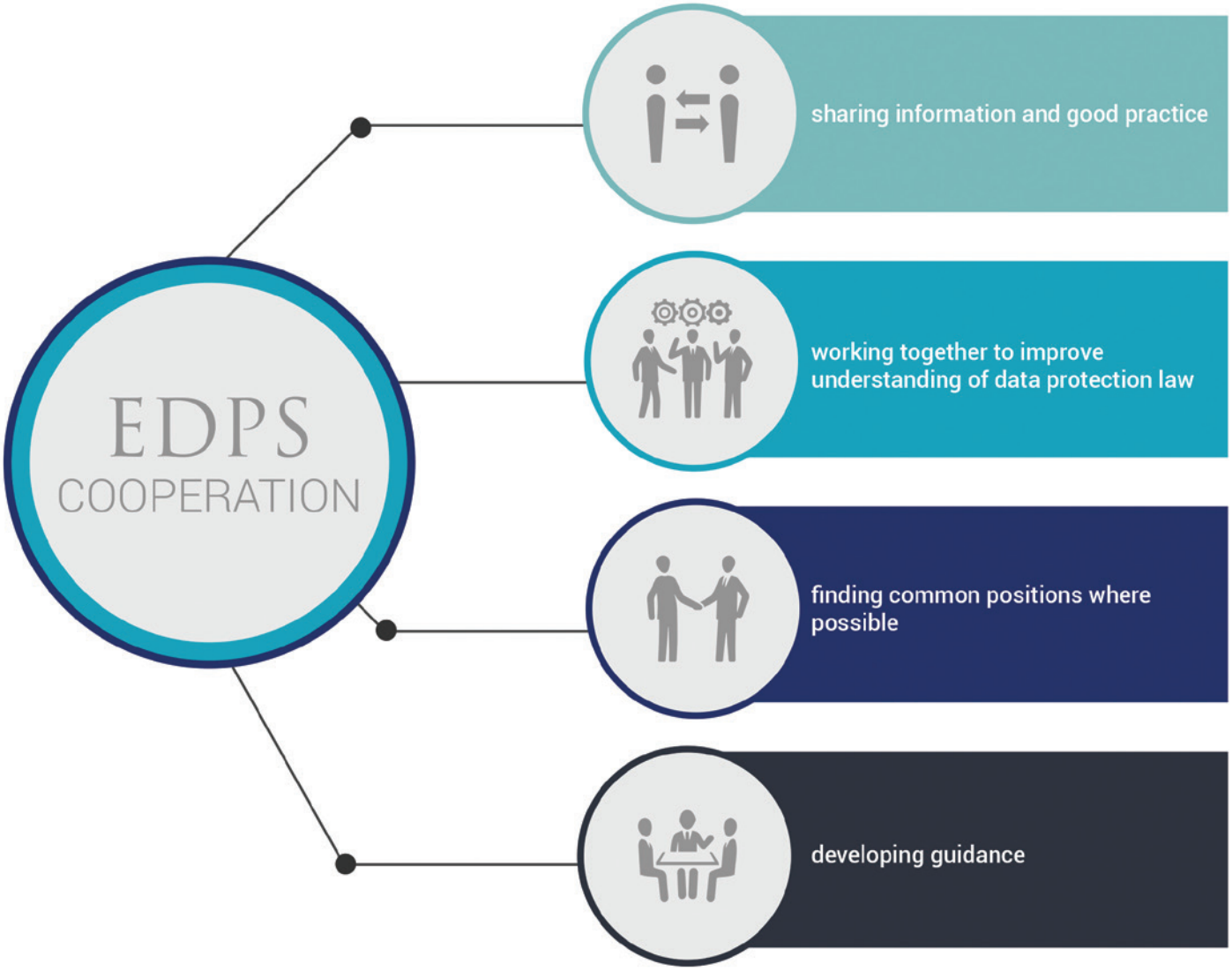
We will continue to follow relevant discussions and developments in the OECD, in cooperation with the European Commission and other participating EU DPAs.

International Organisations Workshop

Generating and fostering global partnerships in the field of data protection is a priority for the EDPS. One of the ways in which we do this is by co-organising a yearly workshop dedicated to data protection within international organisations. The workshop is a forum for the exchange of experiences and views on the most pressing issues in data protection faced by international organisations all over the world. In 2019, we collaborated with the Organisation for Economic Cooperation and Development (OECD) to organise the workshop.

The size and the relevance of this event has been growing since the first edition in 2005. This confirms the need for a platform for international organisations to engage, share best practices and discuss unsolved dilemmas, and demonstrates the increasing awareness of the importance of ensuring strong safeguards for personal data. In 2019, we welcomed a record number of more than 90 participants representing more than 40 different organisations, including representatives from the United Nations.

Over the course of two days, participants discussed the challenges they face in developing a data protection policy in their respective organisations. These included issues relating to web service and social media use, software contract negotiation and effective risk



assessment. Discussions included a wealth of advice and practical solutions for international organisations to put into practice.

Our colleagues in international organisations are working hard to develop strong safeguards for personal data within their organisations, and they were keen to exchange views on present and future challenges. One of the most important lessons that we took away from this workshop is that the development of robust data protection standards is, and will continue to be, a joint effort. The EDPS will continue to support the efforts of international organisations and contribute to increasing global cooperation.

The International Conference of Data Protection and Privacy Commissioners

The 2019 International Conference of Data Protection and Privacy Commissioners (ICDPPC) took place in Tirana, Albania, from 20-24 October 2019. As in past years, the conference was split into two sessions: the Closed Session, attended by ICDPPC members, and the Open session, attended by all interested participants.

The main aim of the Closed Session was to define a framework for future cooperation that would continue to strengthen the group's position as an effective international forum. The group therefore agreed on a policy strategy based on three pillars:

1. evolution toward global frameworks and standards;

2. greater enforcement cooperation;

3. identifying priority policy themes.

The group also confirmed three strategic priorities:

1. advancing global privacy in a digital age, confirming a move towards a global regulatory environment;

2. maximising the conference's voice and influence, notably in enhancing the conference's role in digital policy and strengthening relationships with other international bodies and networks. Work on this priority will be chaired by the EDPS;

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

The group also agreed on a new name for the ICDPPC: the Global Privacy Assembly (GPA).

The Closed Session included a detailed discussion on Artificial Intelligence, building on the 2018 resolution on this topic, and produced five new resolutions:

- on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement;
- on privacy as a fundamental human right and precondition for exercising other fundamental rights;
- to support and facilitate regulatory cooperation between data protection authorities and consumer protection and competition authorities to achieve clear and consistently high standards of data protection in the Digital Economy;
- to address the role of human error in personal data breaches;
- on social media and violent extremist content online.

A number of authorities, including the EDPS, abstained from voting on the last of these resolutions.

The Open Session of the conference focused on data protection convergence and the concept of accountability as a global standard for data protection. This included a panel moderated by Assistant Supervisor Wojciech Wiewiórowski, which focused on understanding how regulators in the different spheres of competition and data protection law are beginning to work together in practice.

As is tradition, several side events took place during the week. In order to ensure that the international discussion on Digital Ethics - the theme of the 2018 conference co-organised by the EDPS in Brussels - continues to move forward, we organised a side event focused on one of the less well-known consequences of the digital revolution: the climate crisis and its impact on digital rights.

The event aimed to build on a discussion initiated in one of our #DebatingEthics Conversations podcasts, in which we addressed the relatively under-explored consequences of the digital revolution for climate change and human rights. It focused on whether universal rights to privacy will be able to withstand the consequences of climate change over the coming years, with regard to increasing migration flows.

We look forward to continued international cooperation through the increasingly valuable forum. The 2020 edition of the conference will take place in October 2020, in Mexico City.

Digital Ethics: beyond the 2018 International Conference

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 can do this is by fostering a continuous debate on what is ethical in the digital sphere. The EDPS has invested considerable effort in this endeavour, succeeding in launching a global debate on Digital Ethics at the 2018 International Conference of Data Protection and Privacy Commissioners. Our focus for 2019 was therefore 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.

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 (AI), Ethics and Data Protection in 2018 has ensured that discussion about Digital Ethics remains firmly on the international agenda.

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.

The Berlin Group visits Brussels

On 10 - 11 October 2019, the EDPS hosted the meeting of the International Working Group on Data Protection in Telecommunications (IWGDPT) for the first time. The group was established in 1983 and is chaired by the Berlin Data Protection Authority. It is therefore known informally as the Berlin Group.

During the meeting, the group decided to change their name, replacing Telecommunications with Technology to reflect the much broader focus of the group over the past few years. In their recent meetings, for example, the group has adopted working papers on Artificial Intelligence, Smart Devices and Online Services for Children.

As the Berlin Group includes representatives from civil society organisations and other experts from around the world, it is an excellent forum in which to facilitate discussions between data protection authorities and other concerned parties on the data protection and privacy risks of certain initiatives. For example, the Group plans to look into payment systems based on cryptocurrencies. Some organisations plan for large-scale rollouts of such technology, which may place even more detailed and precise personal data into the hands of the most data-hungry organisations.

During the meeting, the EDPS also updated the Berlin Group on our most recent activities. Our IT Policy unit presented TechDispatch, which provides an introduction to new technologies (see section 3.2.9) and their potential data protection issues, as well as the Website Evidence Collector. This new piece of software, developed by the EDPS, helps web developers, data protection experts and others to improve their data protection compliance (see section 3.2.8).

The Israeli Data Protection Authority will host the next meeting of the Berlin group in Tel Aviv, on 4 - 5 March 2020.

The Ibero-American Conference

Starting on 13 November 2019, the Ibero-American Data Protection Network (RIPD) and the Spanish Agency for International Development Cooperation (AECID) held a three-day conference in Montevideo, Uruguay, entitled *One year of application of the General Data Protection Regulation (GDPR)*.

In addition to a representative from the EDPS, those attending included representatives from Ibero-American data protection authorities, the US Federal Trade Commission, the European Commission, big tech companies and civil rights NGOs, as well as data protection professionals and members of academia.

The event provided a comprehensive overview of data protection-related legal developments in Ibero-American countries. With the GDPR now in place, Ibero-American regulators have been using it as a comparative standard for their own legislation. Many countries without a specific data protection regulation are in the process of drafting one, while others are updating their current legislation based on the main principles of the GDPR, promoting concepts such as accountability and the right to data portability.

The Spanish Data Protection Authority (AEPD), which provides the Secretariat for the network, plans to follow up this successful conference with a seminar on Artificial Intelligence and Ethics in 2020.

4. Court Cases

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

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

Rulings made on cases relating to data protection help us to interpret data protection law and to ensure that the fundamental right to privacy and data protection is fully respected.

We followed closely all court cases relating to the protection of personal data in 2019, and were directly involved in one case.

4.1 DATA RETENTION UNDER SCRUTINY

Confidentiality of communications is essential for the functioning of a modern, democratic society. On 9-10 September 2019, the EDPS was invited to appear before the CJEU as part of a joint hearing in a number of cases, primarily relating to the retention of telecommunications data and to regimes governing access to electronic communications data by State authorities.

All parties invited to the hearing were asked to answer several questions, aimed in particular at clarifying the scope of EU law in relation to data retention practices. In addition, the EDPS was invited to answer specific questions with a strong technical component.

Our oral pleading is available on our website. We will continue to follow developments relating to this case in 2020.

5. Transparency and Access to Documents

As an EU institution and according to our Rules of Procedure, the EDPS is subject to Regulation 1049/2001, on public access to documents. Within the EDPS, the person responsible for handling these requests is a designated legal officer. In their role as Transparency Officer, they collaborate with the relevant staff members in order to respond appropriately to the request.

After a decrease in the number of public access requests received for documents held by the EDPS in 2018, the number increased again this year, rising from 9 requests in 2018 to 20 requests in 2019. In 5 of these cases, we also received confirmatory applications. In all cases where documents could be identified, the requested documents were either fully or partially disclosed.

We remain fully committed to increasing the transparency and accountability of our work and aim to update our website, and our public register in particular, with relevant documents and information on a regular basis.

6. The Secretariat

6.1 INFORMATION AND COMMUNICATION

Public interest and engagement with data protection and the work of data protection authorities (DPAs) only continues to grow. The EDPS Information and Communication team must therefore ensure that EDPS activities and messages reach the relevant audiences at the right time.

The role of the EDPS Information and Communication team is set out in the EDPS Strategy 2015-2019. This commits us to making technical issues more accessible for non-experts and to communicating in a transparent manner, appropriate for the relevant audiences.

As 2019 was the last year of the mandate, our efforts focused on consolidating the work carried out over the past five years. We continued our efforts to improve our established communication channels in preparation for the new mandate and continued to build on the success of our recent rebranding efforts to reinforce the image of the EDPS as a respected, international leader in the data protection field.

6.1.1 Online media

Website

In 2017, we launched our new website. Since then, we have continued to make improvements to it, by adding new features and improving the design. In response to stakeholder feedback, we have focused in particular on the homepage, with the aim of providing the best user experience possible and ensuring that all visitors to the website are easily able to find the information they need.

We are also working to develop more accessible and engaging formats for our online publications. In 2019, we introduced user-friendly HTML versions of important publications, ensuring that they could be easily read on any type of electronic device. We also began working on plans for the publication of the EDPS Strategy for the new mandate. This will be available not only in PDF, but in an interactive webpage format, in an effort to make it more appealing and accessible to a wider audience.

In an effort to respond to increased public interest in data protection, we also started producing podcasts, all of which are available on the EDPS website. These offer important in-depth information about current data protection and privacy issues, framed in a more relaxed and conversational format. It also gives listeners the chance to get to grips with the kind of work EDPS staff do on a daily basis, as well as to listen to the opinions of external experts. A more extensive programme of podcasts is planned for 2020.

Social Media

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

LinkedIn has now overtaken Twitter (@EU_EDPS) as our most influential social media tool, but our presence on both platforms continues to grow steadily. Though we published fewer videos in 2019 than we did in 2018, the number of followers on the EDPS YouTube channel has also increased.

Our growing global influence, along with our efforts to implement an effective social media strategy, have helped us to continue expanding our influence and reach online. Through these tools, we are able to reach an increasingly diverse and global audience. Our latest tweets are always available to view on the EDPS homepage.

EDPS blog

The EDPS blog is a platform through which the Supervisor, the Assistant Supervisor and the Director are able to communicate on a more personal level about their thoughts, opinions and activities, as well as the work of the institution in general. It has now been active for over three years and has established itself as an essential EDPS communication tool.

At the beginning of the new EDPS mandate in December 2019, it was decided to open the blog up to Heads of Unit. This will allow us to present a wider range of perspectives on all things data protection. The blog is easily found on the homepage of the website where a short extract from the most recent blogpost is always displayed.

In 2019 we published 17 blogposts on a range of different subjects. These included EDPS meetings with Data Protection Officers (DPOs), workshops with external organisations and insights into new technologies. All of our blogposts were promoted through our social media channels and many of them also received media attention.

6.1.2 Events and publications

A new era in data protection: Reflections on the 2015-2019 EDPS mandate

December 2019 marked the end of one EDPS mandate and the beginning of a new one, with former Assistant Supervisor Wojciech Wiewiórowski taking over as EDPS. To demonstrate the progress made towards achieving the goals we set in the EDPS Strategy 2015-2019, the EDPS published a comprehensive review of our work during the mandate, outlining our achievements, alongside those of the data protection community in general, and highlighting areas in which work must continue.

The publication, for which an Executive Summary is also available, covers important achievements and notable events such as EDPS contributions to the General Data Protection Regulation and Regulation 2018/1725 and EDPS work on Digital Ethics and accountability, among many other things.

To close the mandate, we invited stakeholders to an event, at which we launched the publication, on 3 December 2019. The event included speeches from Commissioner Věra Jourová and BEUC director Monique Goyens, as well as newly-elected EDPS Wojciech Wiewiórowski, who served as Assistant Supervisor throughout the 2015-2019 mandate.

@EU_EDPS

#EDPS @W_Wiewiorowski presents achievements from a pivotal 5 years for data protection. #EDPS Strategy 'Leading by Example' launched debate and strengthened cooperation among global actors in #competition law, #DigitalEthics, online disinformation & manipulation & more

EU Open Day 2019

Every year, the EU institutions celebrate Europe Day by opening their doors to all members of the public. This year's EU Open Day took place on 4 May 2019, providing the EU institutions with an opportunity to increase the transparency of their work and to educate people on the EU's activities. The EDPS participates every year, in an effort to increase general public awareness of our role and data protection in general.

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

With public awareness about privacy and data protection at an all-time high, the increased interest in data protection and the work of the EDPS was both understandable and encouraging. We look forward to welcoming even more people to our stand in 2020.

Data Protection Day 2019

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

Each year, to mark the occasion, the EDPS trainees organise a lunchtime conference, aimed at engaging young people, specifically other trainees working for the EU institutions, to engage with an important data protection issue.

The 2019 conference was entitled *Big Banking is Watching You*, and focused on the protection of privacy and personal data in online payments and transactions. Both the late EDPS Giovanni Buttarelli and Assistant Supervisor Wojciech Wiewiórowski participated in the conference, which also featured presentations from the worlds of finance, cryptocurrency and policy, among others.

Newsletter

The EDPS Newsletter was revamped mid-2017, and has continued to grow in popularity ever since. The new format means that it is now more accessible and user-friendly on all digital platforms and, by publishing more frequently, we are able to ensure that our readers are kept up-to-date on our latest activities.

In 2019, we published ten editions of the EDPS Newsletter. These included our January special edition, in which we highlighted some of our less high-profile activities from 2018. Other popular topics we covered during the year included data protection in the European Parliament elections, the EDPS investigation into IT contracts held by the EU institutions, and the appointment of Wojciech Wiewiórowski as the new European Data Protection Supervisor.

In May 2019, we carried out a survey of Newsletter readers, aimed at better understanding the needs of our readers. We will continue to make improvements to the Newsletter in 2020 in an effort to respond to these needs. Meanwhile, our mailing list continues to grow. This serves as a constant reminder of the importance and relevance of the Newsletter as a communications tool.

6.1.3 External relations

Media relations

We issued 14 press releases and statements in 2019. This is an increase on 2018 and illustrates the growing demand for information on developments in data protection, as well as the ever-increasing influence of our work. All of our press releases are published on the EDPS website, distributed to our network of journalists and other interested parties and published on the EU Newsroom website. Translations in French and German are also now available.

In addition to our press releases, we received 102 formal requests from European and international press on a wide variety of topics.

One activity on which we received significant press coverage during the year is our investigations, both into EU institution contracts with Microsoft and into the European Parliament's election activities. Other notable events that garnered a considerable degree of press attention included the regrettable passing of the EDPS Giovanni Buttarelli and the appointment of Wojciech Wiewiórowski as the new Supervisor for the 2019-2024 mandate.

Study visits

In 2019, we hosted 14 study visits to the EDPS. As the profile of data protection has increased, so has interest in our work. Though we would like to host every group that expresses an interest in the EDPS and what we are doing, our high workload and the limited space available to host these visits forced us to be a bit more selective.

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

Information requests

The number of public requests for information received by the EDPS decreased slightly in 2019, but remained high. As in past years, the majority of these requests related to matters over which the EDPS has no competence.

We reply to all requests with information relevant to the individual enquiry. This involves referring individuals to the relevant service if their request falls outside our competence, or providing them with the appropriate information to answer their query.

EDPS Information & Communication in 2019: the statistics

Online media:

18 424 Followers on Twitter
464 EDPS tweets
20 357 Followers on LinkedIn
1 666 Followers on YouTube

Events and publications:

4 757 Newsletter subscribers
17 Blogposts

External relations:

14 Press releases
102 Formal requests from press
14 Study visits
455 Public information requests

6.2 ADMINISTRATION, BUDGET AND STAFF

Throughout 2019, the EDPS Human Resources, Budget and Administration (HRBA) Unit has provided support to the Management Board and operational teams at the EDPS. The aim is to ensure 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 members 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.

6.2.1 A growing organisation

The EDPS continues to grow. One of the main reasons for this has been the need to hire more data protection experts, to help us ensure that we are able to take on a range of new roles and perform them competently and effectively. These include providing the secretariat for the European Data Protection Board (EDPB), taking on responsibility for Europol and Eurojust supervision and ensuring that we have the personnel and expertise to carry out the tasks assigned to us under Regulation 2018/1725, as well as covering usual staff turnover.

In addition to this, data protection scandals, new technologies and the new EU data protection framework have led to greater public awareness about data protection rights and obligations. This has led to increased demand for the services of Data Protection Authorities (DPAs), the EDPS included. We therefore need to ensure that we have the resources to respond to these needs appropriately, in order to ensure the protection of individuals' rights.

To respond to these needs, a competition for specialists in data protection was organised in 2018 and completed in 2019. The competition produced a reserve list of 33

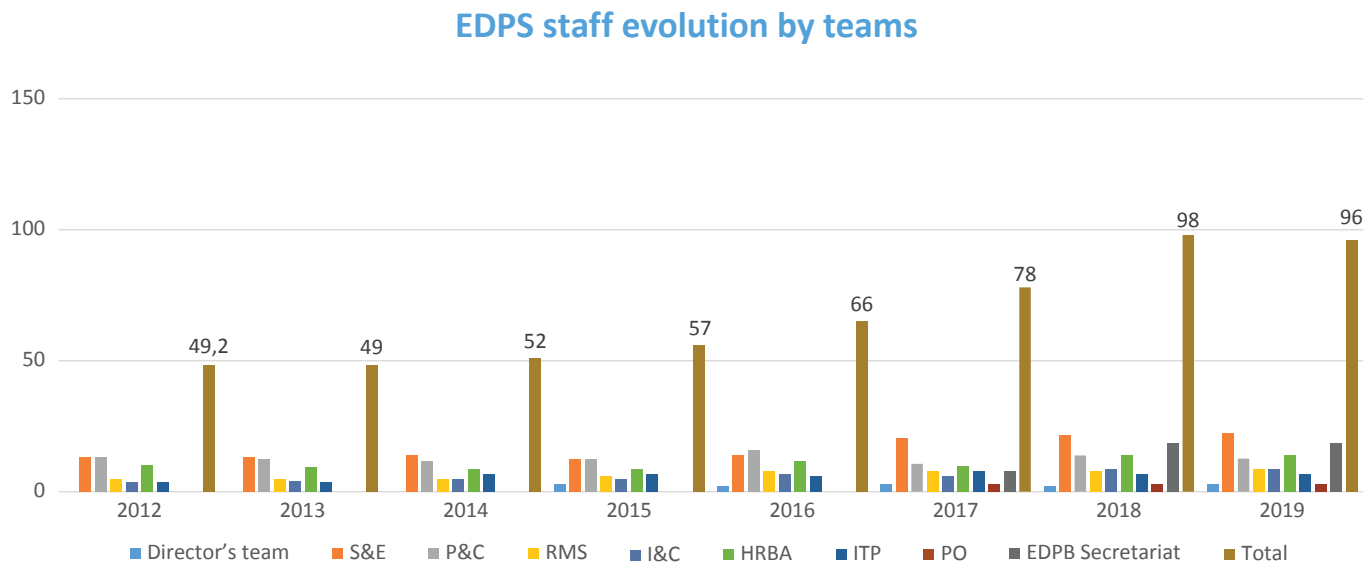


Figure 9. Staff evolution by teams

laureates. We published the list in June 2019 and will use it to recruit new staff members for the EDPS and the EDPB over the coming years.

Our growing number of recruits also presents us with a new challenge: finding office space for them. We therefore began an ongoing project focused on maximising the office space already available to us, as well as acquiring new space. Further progress in this area is expected over the coming months.

6.2.2 Learning and Development

In 2019, we launched our 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, in addition to helping to find specific solutions to professional challenges. Our own internal coach conducts the sessions.

Another initiative organised by the HRBA unit in 2019 was the HR teasers. These are short presentations given over lunchtimes, covering topics of interest to new colleagues. They aim to help new colleagues better understand the role and function of Human Resources within the institution, which, in turn, improves everyday workplace proceedings. The teasers cover topics such as internal IT systems and processes, procurement, service level agreements (SLAs), a Q&A for newcomers and the EU learning and development platform.

We also continued work on a pilot secondment programme in 2019. The General Data Protection Regulation (GDPR) entrusts the EDPB with the task of promoting the exchange of information, practices and common training programmes between supervisory authorities. One way of doing this is through the temporary exchange of personnel. The EDPS HRBA unit has significant experience in the organisation of similar exchanges, which is why we proposed facilitating the process, involving the exchange of staff members between DPAs themselves or between a DPA and the EDPB secretariat. The draft programme was discussed at a meeting between Human Resources and Learning and Development representatives from the DPAs in September 2018, and the first edition of the programme is due to take place in 2020.

6.2.3 Going paperless

For environmental and efficiency reasons, we have taken the first steps towards becoming a paperless institution. Our first project concerns the payment of invoices.

The decision to implement a paperless tool was taken in November 2018 and implementation was finalised at the end of 2019. The tool is called Speedwell and was created by the European Research Council Executive Agency (ERCEA). It involves less printing and archiving and makes it easier to verify transactions, leading to increased productivity, better quality work processes and an eco-friendly approach to the payment of invoices.

Over the course of 2019 we also carried out various trial staff selection procedures with reduced paper consumption. Testing is already underway on how to share documents with selection panel members electronically, yet securely, as well as on paperless interviews.

6.2.4 Welcome Day for newcomers

The HRBA unit is constantly looking for ways to improve, especially where newcomers are concerned. Newcomers at the EDPS have always received a welcome package on their first day, which includes a schedule of welcome meetings with certain colleagues. Although this works well, in 2019 we decided to adjust the structure of this welcome to include participation in a *Newcomers' Welcome Day* during the first weeks following their arrival. This Welcome Day takes the form of a meeting in which each key colleague gives a presentation to the newcomers. This improves the overall efficiency of the welcome process.

6.2.5 Finance and Procurement

The Procurement Professionalisation Project (PPP) began in 2018, with the aim of improving the efficiency of our financial processes and ensuring compliance with the relevant financial rules. In 2019, we developed the project further through:

- the nomination of colleagues to take responsibility for various financial tasks in the different EDPS units and sectors;
- drafting a new procurement process guide, covering the specific responsibilities relating to each financial role, and implementing an electronic workflow in the Case Management System (CMS), the official EDPS electronic repository;
- the establishment of a procurement plan, to be carried out in parallel with the draft budget exercise.

Colleagues nominated to take on financial roles in the different EDPS units and sectors will be trained in January 2020. This will enable us to ensure an institution-wide implementation of this new work procedure as soon as possible.

The EDPS has also taken steps to benefit from the eTendering platform provided by the EU Publications Office and initiated the process to allow electronic submissions of Tenders through the *eSubmission* system provided by European Commission's Directorate General for Informatics (DG DIGIT). Progress in both areas is expected in the first quarter of 2020.

As a small institution, the EDPS is heavily reliant on single tender procedures for very low value purchases, as well as Inter-institutional Framework Contracts, to ensure efficiency. In addition to this, the Procurement team launched the following competitive procedures in 2019:

- Open Procedure EDPS/2019/02: Studies on the implications of several GDPR provisions, case laws and other laws having an impact on data protection;
- Two Low Value Negotiated Procedures concerning the production of the European Data Protection Board's 2019 Annual Report and the memorial for the late EDPS Giovanni Buttarelli;
- Middle Value Negotiated Procedure EDPS/2019/01: Coaching to carry out data protection audits of mobile apps provided by EU institutions and bodies.

We also identified several EDPS purchases as *recurrent*. We will therefore start a competitive procedure for these cases in 2020.

In addition, we have prepared several decisions and work procedures with the aim of defining a financial framework that is more suited to a fast-growing organisation such as the EDPS. This includes a decision on the registration and documentation of deviations, protocols on team-building events and a decision on the reimbursement of travel and subsistence expenses incurred by job applicants.

Budget

In 2019, the EDPS was allocated a budget of EUR 16 638 572. This represents an increase of 15.15% compared to the 2018 budget.

The overall increase was mainly due to the impact of the new tasks appointed to the EDPS in Regulation 2018/1725 and the necessary expansion of the EDPB, for which the EDPS provides an independent secretariat.

Regarding budget implementation, the overall rate in commitment appropriations amounted to 92%. The main obstacles preventing us from achieving a higher implementation rate were unforeseen delays in acquiring additional office space and that estimations for the 2019 budget for the EDPB had been prepared before the secretariat was operational, making it difficult for us to predict their budgetary needs.

7. The Data Protection Officer at the EDPS

7.1 THE DPO AT THE EDPS

The focus of the DPO office at the EDPS in 2019 has been to ensure a smooth transition to the new rules for the EU institutions, set out in Regulation 2018/1725, while always keeping the role and mission of the EDPS in mind.

We are a small institution, tasked with responsibilities that influence the lives, dignity and fundamental rights of all individuals in the EU, as well as their relationships with other people, private entities and public administration. In addition to this, we now operate in an environment increasingly dominated by new technologies, many of which collect and process personal data. In this context, public institutions such as the EDPS must ensure that, in everything they do, they put the interests and rights of the individual first.

This objective cannot be achieved without increasing our focus on accountability. We therefore aim to ensure that all EDPS staff take responsibility for ensuring that the protection of individuals and their data is the primary concern in all activities. This includes adopting a *data protection by design* approach to data processing.

As the principal authority on data protection in the EU institutions, we seek to lead by example. This will continue to be the underlying mission of the DPO office for the years to come.

7.2 PUTTING ACCOUNTABILITY INTO PRACTICE

Transparency has been a significant focus of our work over the past year. This has involved completing all data protection notices for the tasks listed in the EDPS Register of activities.

We have also put in place new procedures to better deal with requests from individuals to exercise their data protection rights. One essential requirement for carrying out these requests is to be able to establish the link between the person submitting the request and their personal data. We therefore decided to update the relevant EDPS procedure to better facilitate this, bringing it in line with the requirements of the Regulation 2018/1725.

In addition, in some EDPS activities transparency needs to be balanced with other individual and public interests. We therefore published the EDPS Decision on the restriction of certain data subject rights, as is required by Article 25 of Regulation 2018/1725.

Dealing with different contexts and situations means that ensuring transparency and accountability is always *work in progress* and a constant learning process. Our ongoing consolidation of procedures relating to the management of individuals' rights ensures that we are accountable *by design* and in practice.

7.3 ADVISING THE INSTITUTION

One of the main tasks of a DPO is to advise their institution on data protection policies and practices. For example, Regulation 2018/1725 requires organisations acting as controllers of personal data to select contractors, who are to act as processors of personal data, by carefully assessing the ability of the contractor to comply with data protection rules. The rules also require that controllers bind their contractors through agreement to specific safeguards, including ad-hoc contractual provisions.

The DPO Office at the EDPS has provided relevant advice on several occasions in which the EDPS has faced difficulties in finding suitable service providers able to offer these guarantees. These difficulties generally arise because service providers impose their own, unilateral, terms.

We also had the opportunity to advise the institution in reviewing certain internal rules and procedures, such as those on whistleblowing, as well as service level agreements (SLAs) and memoranda of understanding with other institutions that provide or share their services with the EDPS.

7.4 ENQUIRIES AND COMPLAINTS

This year we received two requests from individuals for access to their personal data. Each posed different challenges.

For one request, we concluded that, based on the information provided, no means were available to verify

the identity of an individual who claimed to have browsed the EDPS website. The other request required a substantial investment of resources. This was because of the scope of the request, the amount of personal data requested and the need to assess whether other people's rights were at risk and, where this was the case, to protect them.

Surprisingly, after peaking in 2018, the year in which Regulation 2018/1725 entered into force, the number of individual requests received by the EDPS decreased remarkably in 2019. We believe that the likely cause of this decrease may be the improvements made to ensure compliance and accountability since the new rules came into force. Practical examples of this include the improved management of cookies and personal data on our website, as well as having put in place a clear data protection policy for the organisation of events.

7.5 AWARENESS-RAISING WITHIN THE EDPS

All new colleagues who join the EDPS meet the EDPS DPO and Assistant DPO within their first month at the institution. This meeting is an opportunity for us to provide an induction to personal data protection, adapted to the educational and professional background of individual participants.

The EDPS welcome programme for new colleagues was revamped for 2019, and the DPO office took the opportunity to update our contribution, including an introduction on the applicable data protection law and placing greater emphasis on the role EDPS staff members play in ensuring the protection of individuals and their personal data. The prevailing message is that every staff member must be accountable.

Training sessions were also made more practical, teaching new recruits how to identify and react to a personal data breach, or where to find internal data protection resources, for example. The same information was offered to all existing staff members in an ad-hoc session.

7.6 COLLABORATION WITH DPOS FROM THE EU INSTITUTIONS

Meetings between DPOs of the EU institutions, bodies and agencies and the EDPS are becoming an increasingly valuable source of expertise and exchange, providing an opportunity to discuss best practice with colleagues.

In 2019, the EDPS participated in both the DPO meeting in Frankfurt, organised by the European Insurance and Occupational Pensions Authority (EIOPA), and the DPO meeting in Florence, hosted by the Historical Archives of the EU (see section 3.2.1). At these meetings, DPOs have the opportunity to work together on themes such as the transfer of personal data to third countries or resources for data protection training, putting data protection theory into practice.

The procurement and use of IT systems, particularly those that are cloud-based, has been a particular focus of DPO attention in 2019 (see section 3.2.4), with procurement having been one of the topics covered at the DPO meetings. Recent EDPS investigations and international developments have exposed the need to establish a new status quo, in which providers no longer impose conditions unilaterally. This would empower organisations to manage IT systems in full compliance with data protection law.

Annex A - Legal framework

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

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

Other relevant EU acts on data protection are:

- Directive 95/46/EC, which was replaced by Regulation 2016/679, the General Data Protection Regulation (GDPR), on 25 May 2018. The GDPR lays down a general framework for data protection law in the Member States;
- Directive 2002/58/EC on privacy and electronic communications (as amended by Directive 2009/136);
- Directive on data protection in the police and justice sectors.

A new Regulation on privacy and electronic communications (ePrivacy) is currently under negotiation.

Background

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms provides for a right to respect for private and family life, subject to restrictions allowed only under certain conditions.

However, in 1981 it was considered necessary to adopt a separate convention on data protection, in order to develop a positive and structural approach to the protection of fundamental rights and freedoms which may be affected by the processing of personal data in a modern society. The convention, also known as Convention 108, has been ratified by more than 40 Member States of the Council of Europe, including all EU Member States. Convention 108 will be amended by its Protocol (CETS No 223) upon its entry into force.

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

On 6 April 2016, the EU agreed to a major reform of its data protection framework, adopting the GDPR to replace the old Directive. The GDPR is an essential step forward in strengthening citizens' fundamental rights in the digital age. It focuses on reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards.

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

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

Regulation (EC) No 45/2001

Taking a closer look at Regulation 45/2001, it should be noted first that, according to Article 3(1), it applies to the *processing of personal data by Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which are within the scope of Community law*. However, since the entry into force of the Lisbon Treaty and the abolition of the pillar structure – as a result of which references to *Community institutions* and *Community law* have become outdated – the Regulation in principle covers all EU institutions and bodies, except to the extent that other EU acts 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 only became applicable to the processing of personal data by Eurojust from 12 December 2019 and it does not apply to the processing of operational personal data by Europol and the European Public Prosecutor's Office, nor to the processing of personal data as part of activities referred to in Articles 42(1), 43 and 44 TEU, such as activities carried out within the framework of the common security and defence policy. In addition, only Article 3 and Chapter IX of the Regulation apply to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities of judicial cooperation in criminal matters or police cooperation.

The definitions and the substance of the Regulation closely follow the approach of the GDPR. It could be said that Regulation (EC) No 2018/1725 is the implementation of the GDPR at EU institution level. The structure of Regulation 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 develop further (see section 3.2.1).

Tasks and powers of the EDPS

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

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

Some tasks are of a special nature. The task of advising the Commission and other EU institutions about new legislation — highlighted in Article 28(2) of Regulation 45/2001 and Article 42 of Regulation 2018/1725 by a formal obligation for the Commission to consult the EDPS when it adopts a legislative proposal relating to the protection of personal data — also relates to draft directives and other measures that are designed to apply at national level or to be implemented in national law. This is a strategic task that allows the EDPS to look at privacy implications at an early stage and to discuss any possible alternatives, including in areas that used to be part of the former *third pillar* (police and judicial cooperation in criminal matters). Monitoring relevant developments which may have an impact on the protection of personal data and intervening in cases before the Court of Justice are also important tasks. In addition, pursuant to Article 42(2) of Regulation 2018/1725, the European Commission may consult the European Data Protection Board (EDPB), established to advise the European Commission and to develop harmonised policies under the GDPR, on proposals which are of *particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data*. In such cases, the EDPB and the EDPS *coordinate their work with a view to issuing a joint opinion*.

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

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

Article 41 - Information and consultation

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

2. The Union institutions and bodies shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in Article 25.

Article 42 - Legislative consultation

1. The Commission shall, following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the European Data Protection Supervisor where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

2. Where an act referred to in paragraph 1 is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission may also consult the European Data Protection Board. In such cases the European Data Protection Supervisor and the European Data Protection Board shall coordinate their work with a view to issuing a joint opinion.

3. The advice referred to in paragraphs 1 and 2 shall be provided in writing within a period of up to eight weeks of receipt of the request for consultation referred to in paragraphs 1 and 2. In urgent cases, or if otherwise appropriate, the Commission may shorten the deadline.

4. This Article shall not apply where the Commission is required, pursuant to Regulation (EU) 2016/679, to consult the European Data Protection Board.

Article 52 - European Data Protection Supervisor

1. The European Data Protection Supervisor is hereby established.

2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies.

3. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and of any other Union act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Union institution or body, and for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data. To those ends, the European Data Protection Supervisor shall fulfil the tasks set out in Article 57 and exercise the powers granted in Article 58.

4. Regulation (EC) No 1049/2001 shall apply to documents held by the European Data Protection Supervisor. The European Data Protection Supervisor shall adopt detailed rules for applying Regulation (EC) No 1049/2001 with regard to those documents.

Article 57 - Tasks

1. Without prejudice to other tasks set out under this Regulation, the European Data Protection Supervisor shall:

   a) monitor and enforce the application of this Regulation by Union institutions and bodies, with the exception of the processing of personal data by the Court of Justice acting in its judicial capacity;

b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

c) promote the awareness of controllers and processors of their obligations under this Regulation;

d) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the national supervisory authorities to that end;

e) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 67, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

f) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

g) advise, on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;

h) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

i) adopt standard contractual clauses referred to in Article 29(8) and in point (c) of Article 48(2);

j) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39(4);

k) participate in the activities of the European Data Protection Board;

l) provide the secretariat for the European Data Protection Board, in accordance with Article 75 of Regulation (EU) 2016/679;

m) give advice on the processing referred to in Article 40(2);

n) authorise contractual clauses and provisions referred to in Article 48(3);

o) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2);

p) fulfil any other tasks related to the protection of personal data; and

q) establish his or her Rules of Procedure.

2. The European Data Protection Supervisor shall facilitate the submission of complaints referred to in point (e) of paragraph 1 by a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of the European Data Protection Supervisor shall be free of charge for the data subject.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the European Data Protection Supervisor may refuse to act on the request. The European Data Protection Supervisor shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58 - Powers

1. The European Data Protection Supervisor shall have the following investigative powers:

a) to order the controller and the processor to provide any information it requires for the performance of his or her tasks;

b) to carry out investigations in the form of data protection audits;

c) to notify the controller or the processor of an alleged infringement of this Regulation;

d) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of his or her tasks;

e) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union law.

2. The European Data Protection Supervisor shall have the following corrective powers:

a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

c) to refer matters to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;

d) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

e) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

f) to order the controller to communicate a personal data breach to the data subject;

g) to impose a temporary or definitive limitation including a ban on processing;

h) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 18, 19 and 20 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;

i) to impose an administrative fine pursuant to Article 66 in the case of non-compliance by a Union institution or body with one of the measures referred to in points (d) to (h) and (j) of this paragraph, depending on the circumstances of each individual case;

j) to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation.

3. The European Data Protection Supervisor shall have the following authorisation and advisory powers:

a) to advise data subjects in the exercise of their rights;

b) to advise the controller in accordance with the prior consultation procedure referred to in Article 40, and in accordance with Article 41(2);

c) to issue, on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data;

d) to adopt standard data protection clauses referred to in Article 29(8) and in point (c) of Article 48(2);

e) to authorise contractual clauses referred to in point (a) of Article 48(3);

f) to authorise administrative arrangements referred to in point (b) of Article 48(3);

g) to authorise processing operations pursuant to implementing acts adopted under Article 40(4).

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

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

Annex C - List of Data Protection Officers

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

Consumers, Health and Food Executive Agency (CHAFEA)	*Manuel CRESPO OTERO*
European Centre for Disease Prevention and Control (ECDC)	*Andrea IBER*
European Environment Agency (EEA)	*Olivier CORNU*
European Investment Fund (EIF)	*Paolo SINIBALDI*
European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)	*Nayra PEREZ*
European Securities and Markets Authority (ESMA)	*Sophie VUARLOT-DIGNAC*
European Aviation Safety Agency (EASA)	*Geoffrey DEVIN*
Executive Agency for Small and Medium-sized Enterprises (EASME)	*Elke RIVIERE*
Innovation and Networks Executive Agency (INEA)	*Caroline MAION*
European Banking Authority (EBA)	*Joseph MIFSUD*
European Chemicals Agency (ECHA)	*Bo BALDUYCK*
European Research Council Executive Agency (ERCEA)	*Roberta MAGGIO*
Research Executive Agency (REA)	*Maria Francisca BRUNET COMPANY*
European Systemic Risk Board (ESRB)	*Evanthia CHATZILIASI*
Fusion for Energy (ITER)	*Angela BARDENHEWER-RATING*
SESAR Joint Undertaking (SESAR)	*Laura GOMEZ GUTIERREZ*
Electronic Components and Systems for European Leadership (ECSEL)	*Anne SALAÜN*
Clean Sky Joint Undertaking (CLEAN SKY JOINT)	*Bruno MASTANTUONO*
Innovative Medicines Initiative Joint Undertaking (IMI JU)	*Sebastien PECHBERTY*
Fuel Cells & Hydrogen Joint Undertaking (FCH)	*Georgiana BUZNOSU*
European Insurance and Occupations Pensions Authority (EIOPA)	*Catherine COUCKE*
European Police College (CEPOL)	*Ioanna PLIOTA*
European Institute of Innovation and Technology (EIT)	*Nora TOSICS*
European Defence Agency (EDA)	*Clarisse RIBEIRO*
Body of European Regulators for Electronic Communications (BEREC)	*Marco DE SANTIS*
European Union Institute for Security Studies (EUISS)	*Nikolaos CHATZIMICHALAKIS*
European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)	*Encarna GIMENEZ*
Shift2Rail Joint Undertaking (S2R JU)	*Isaac GONZALEZ GARCIA*
Single Resolution Board (SRB)	*Esther BRISBOIS*
Europol (EUROPOL)	*Daniel DREWER*
Bio-Based Industries joint Undertaking (BBI JU)	*Marta CAMPOS ITURRALDE*
European Union's Judicial Cooperation Unit (EUROJUST)	*Diana ALONSO BLAS*

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

Opinions

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

In 2019 the EDPS issued Opinions on the following subjects (date of publication in brackets):

- Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (6 November 2019)
- Negotiating mandate of an Agreement between the EU and Japan for the transfer and use of Passenger Name Record data (25 October 2019)
- Revision of the EU Regulation on service of documents and taking of evidence (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)
- Participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention (2 April 2019)
- Negotiating mandate of an EU-US agreement on cross-border access to electronic evidence (2 April 2019)
- Two legislative proposals relating to combating VAT fraud (14 March 2019)

Formal Comments

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

In 2019 the EDPS issued formal comments on the following subjects (date of publication in brackets):

- Proposals on Regulations establishing the conditions for accessing other EU information systems (ECRIS-TCN, SIS, EES and VIS) for ETIAS purposes (13 March 2019)
- Commission proposal on preventing the dissemination of terrorist content online (12 February 2019)
- Credit servicers, credit purchasers and the recovery of collateral (24 January 2019)
- Return directive recast proposal Art 57(1)(g)of the new regulation (10 January 2019)

Annex E - Speeches by the Supervisor and Assistant Supervisor in 2019

European Parliament

Wojciech Wiewiórowski, Presentation of the EDPS-EDPB Joint Reply on US CLOUD Act and EDPS Opinions 2/2019 and 3/2019, speech before Committee on Civil Liberties, Justice and Home Affairs (LIBE) in European Parliament, Brussels (7 November 2019).

Wojciech Wiewiórowski, Europol Joint Parliamentary Scrutiny Group, speech at European Parliament, Brussels (23 September 2019).

Wojciech Wiewiórowski, Presentation of EDPS Tasks and Activities, speech before the Committee on Civil Liberties, Justice and Home Affairs (LIBE), European Parliament, Brussels (5 September 2019).

Giovanni Buttarelli, Annual Report 2018 speech to LIBE in European Parliament, Brussels (26 February 2019).

European Commission

Wojciech Wiewiórowski, *Security, State of the Art and Certification*, speech during ENISA *Annual Privacy Forum 2019*, Rome, Italy (13-14 June 2019).

Wojciech Wiewiórowski, *Powers and tasks of EDPS and the role of DPO and DPCs under Regulation 2018/1725. Are 70 commandments of Raab and Bennett still valid?*, speech at seminar for DPOs and DPCs from the European Commission on 13th European Data Protection Day, Brussels (28 January 2019).

Other EU Institutions and bodies

Wojciech Wiewiórowski, *Security, State of the Art and Certification*, speech at ENISA Annual Privacy Forum 2019, Rome, Italy (13-14 June 2019).

Giovanni Buttarelli, *The challenges in Privacy by Design*, speech at ENISA Annual Privacy Forum 2019, Rome, Italy (13 June 2019).

Wojciech Wiewiórowski, concluding speech at the ENISA conference *Towards accessing the risk in personal data breaches*, Brussels (4 April 2019).

International Conferences

Wojciech Wiewiórowski, *Role of the DPO in the public institution. National and European perspective*, speech at the *DPO Circle Annual Conference,* Brussels (13 December 2019).

Wojciech Wiewiórowski, *Now for the Stick: Enforcing Data Protection Laws*, lecture during IAPP Europe Data Protection Congress 2019, Brussels (18-21 November 2019).

Wojciech Wiewiórowski, *Challenges for data protection. EU regulatory perspective*, speech at the conference Freedom not Fear 2019, Brussels (8-11 November 2019).

Wojciech Wiewiórowski, *Being Open for Not an Easy Dialog on Global Approach to the Privacy Protection*, speech at the *EU-China Symposium on Data Security and Personal Data Protection*, Brussels (8-11 November 2019).

Wojciech Wiewiórowski, *Follow up to the AI and ethics debate at the 41st Conference in Tirana – From Theory to Practice. Is there a mismatch between the development of tools by the AI tech community, and the goals/demands of the ICDPPC AI Declaration?* and *The Creation of an Independent Authority* at the 41st International Conference of Data Protection and Privacy Commissioners, Tirana, Albania (21-24 October 2019).

Wojciech Wiewiórowski, *Technology as the Challenge for Data Protection Law*, speech at The International Working Group on Data Protection in Telecommunications (Berlin Group), Brussels (10-11 October 2019).

Wojciech Wiewiórowski, *Data Protection 2020-2030 - What's At Stake?*, speech at *Nordic Privacy Arena 2019*, Stockholm, Sweden (23-24 September 2019).

Wojciech Wiewiórowski, *Town Meets Gown: Legal education in interaction with government, business and technological development*, speech at the scientific conference in the scope of the 19th Global Law Deans Forum, Gdansk, Poland (20-22 September 2019).

Wojciech Wiewiórowski, *Controller, processor or ... joint controllers. Public sector perspective*, speech at *Privacy Laws & Business. GDPR's Influence Ripples Around The World*, Cambridge, United Kingdom (1-3 July 2019).

Wojciech Wiewiórowski, *The Role of an Independent Data Protection Supervisory Authority Under GDPR*, speech at *4th European Data Protection Law Summer School: Advancing (with) EU data protection,* Brussels (24-28 June 2019).

Wojciech Wiewiórowski, *Recap on Correct Management of Personal Data*, speech at *Summer ELSA Law School on Data Management: The Data-Centric Week*, Maastricht, The Netherlands (16-23 June).

Wojciech Wiewiórowski, *The 'state of the art' in data protection by design – Current state and future trends*, speech at 10th Internet Privacy Engineering Network (IPEN) workshop, Rome, Italy (12 June 2019).

Giovanni Buttarelli, discussion of state-of-the-art technology for privacy and data protection at 10th Internet Privacy Engineering Network (IPEN) workshop, Rome, Italy (12 June 2019).

Wojciech Wiewiórowski, *Danetyzacja przestrzeni prawnej*, speech at the conference XI Konferencji Bezpieczeństwo w Internecie pt. *Analityka danych*, Warsaw, Poland (6-7 June 2019).

Wojciech Wiewiórowski, *Protection of Personal Data at the Age of Intelligent Artificial Entities*, speech at the conference *Conference: AI Beyond the Hype – Benefits, Challenges and Liabilities*, Edinburgh, United Kingdom (30 May – 1 June 2019).

Giovanni Buttarelli, *Deception by design?*, speech at the 11th Privacy Forum of ISMS Forum, Madrid, Spain (30 May 2019).

Wojciech Wiewiórowski, *International Legal Environment AD 2019. Is GDPR really influential outside of EU?*", speech at the conference *9th European Data Protection Days: 1 Year of GDPR*, Berlin, Germany (20-22 May 2019).

Wojciech Wiewiórowski, *International Impact of the New EU Data Protection* speech at the conference *Ett år med dataskyddsreformen,* Stockholm, Sweden (21 May 2019).

Wojciech Wiewiórowski, *Automated Individual Decision-Making and Profiling under the GDPR*, final lecture of the LL.M course *European Privacy and Data Protection Law*, Brussels (13 May 2019).

Wojciech Wiewiórowski, *Supervision of data protection in public institutions*, speech at the Spring Conference of European Data Protection Authorities *GDPR - One year (g)old standard*, Tbilisi, Georgia (8-10 May 2019).

Wojciech Wiewiórowski, *GDPR: ten months on – EDPS perspective* lecture during the Annual ERA Conference On European Data Protection Law 2019 *Post-GDPR challenges & e-Privacy reforms*, Brussels (28-29 March 2019).

Giovanni Buttarelli, speech at 11th Privacy Forum of ISMS Forum, Madrid, Spain (20 March 2019).

Wojciech Wiewiórowski, *What do stakeholders expect from the Cybersecurity Competence Network Centre pilot projects?*, speech at the workshop *CyberSec4Europe Launch Event,* Brussels (28 February 2019).

Giovanni Buttarelli, report by the EDPS on Europol Supervision at JPSG meeting on Europol, Bucharest, Romania (25 February 2019).

Wojciech Wiewiórowski, *Disinformation campaigns and the political participation of EU citizens*, speech at the workshop *IdeasLab 2019*, Brussels (21-22 February 2019).

Giovanni Buttarelli, speech and closing remarks at the 12th International Computers, Privacy and Data Protection Conference in Brussels (1 February 2019).

Wojciech Wiewiórowski, *New Data Protection Regulation For EU Institutions and Bodies - Another piece of the puzzle*, speech at the international conference *Computers, Privacy and Data Protection (CPDP) 2019. Data Protection and Democracy*, Brussels (30 January – 1 February 2019).

Wojciech Wiewiórowski, *Collective action under the GDPR*, speech during the workshop *Big Data and non-individual/collective action*, Brussels (29 January 2019).

Wojciech Wiewiórowski, *Why Should We Be Used To Profiling*, speech at the conference *Big Banking is watching you: Privacy in a cashless world,* Brussels (28 January 2019).

Wojciech Wiewiórowski, *Supervision over data protection compliance in European institutions, bodies, offices and agencies. Powers and tasks of EDPS*, speech at the conference *Data Protection in European Institutions. Revised data protection Regulation applicable to EU institutions, bodies, offices and agencies*, Brussels (17-18 January 2019).

Other events

Wojciech Wiewiórowski, *Obywatel w sieci Państwa. Usługi typu „Know-Your-Client" w administracji publicznej a kwestie ochrony prywatności*, keynote speech during the conference XXV Forum Teleinformatyki pt. *Polska '25 - strategie i praktyki cyfrowej transformacji*, Miedzeszyn, Poland (26-27 September 2019)

Giovanni Buttarelli, speech at One year of GDPR application: taking stock in the EU and beyond, Brussels (13 June 2019).

Wojciech Wiewiórowski, *GDPR 1 year after its introduction - what has been achieved, what are the implications?*, open lecture at Frankfurt School of Finance & Management, Frankfurt, Germany (17 May 2019).

Wojciech Wiewiórowski, *Ochrona danych osobowych w instytucjach publicznych*, speech during the scientific conference *Rok RODO*, Gdansk, Poland (16 May 2019).

Giovanni Buttarelli, keynote speaker at ASSO DPO 2019, Milan, Italy (9 May 2019).

Giovanni Buttarelli, *Dark patterns in data protection: law, nudging, design and the role of technology* speech at Legal Design Roundtable, Brussels (29 April 2019).

Wojciech Wiewiórowski, *Konosament a blockchain. Możliwości wykorzystania technologii rozproszonego rejestru dla celów „elektronicznego indosu" przy przenoszeniu praw z papierów wartościowych na zlecenie*, speech during the conference VIII Ogólnopolskiej Konferencji Prawa Morskiego *Przewóz ładunku drogą morską*, Gdańsk, Poland (11 April 2019).

Wojciech Wiewiórowski, *Konosament a blockchain. Możliwości wykorzystania technologii rozproszonego rejestru dla celów „elektronicznego indosu" przy przenoszeniu praw z papierów wartościowych na zlecenie*, speech during the conference *V Forum Prawa Mediów Elektronicznych. Blockchain*, Opole, Poland (9-10 April 2019).

Giovanni Buttarelli, opening remarks at *Europe Votes 2019: How to Unmask and Fight Online Manipulation*, Brussels (11 February 2019).

Giovanni Buttarelli, *Awareness and Responsibility - Ethics, accountability, effectiveness and efficacy: the properties of GDPR*, speech at DIBATTITO GDPR - Consapevolezza e responsabilizzazione at the Italian Chamber of Deputies, Rome, Italy (4 February 2019).

Wojciech Wiewiórowski, *Common Roots and Different Paths for Privacy by Design*, speech at 9th Internet Privacy Engineering Network (IPEN) workshop, Brussels (28 January 2019).

Giovanni Buttarelli, speech at Conference on AI, Ethics and Law, Athens, Greece (25 January 2019).

Giovanni Buttarelli, *New Technology as a Disruptive Global Force*, speech at Youth & Leaders' Summit, Paris, France (21 January 2019).

Annex F - Composition of EDPS Secretariat

Director and Private Office

Leonardo CERVERA NAVAS
Director

Christian D'CUNHA
Head of Private Office of the EDPS

Ernani CERASARO
Policy Administrative Assistant

Anna COLAPS
Policy Assistant

Achim KLABUNDE
Advisor to the Supervisor

Sylvie PICARD
Internal Control Coordinator

Maria José SALAS MORENO
Administrative Assistant

Supervision and Enforcement

Delphine HAROU
Head of Unit

Petra CANDELIER
Head of Complaints and Litigation

Owe LANGFELDT
Head of Audits

Ute KALLENBERGER
Head of Inspections

Bénédicte RAEVENS
Head of EUROPOL Supervision

Stephen ANDREWS
Supervision & Enforcement Assistant

Guillaume BYK
Legal Officer

Evanthia CHATZILIASI*
Legal Officer

Constantin CHIRA-PASCANUT
Legal Officer

Graça COSTA
Legal Officer

Fanny COUDERT
Legal Officer

Andrew CURRY*
Legal Officer/Seconded National Expert

Elena FIERRO*
Legal Officer

Barbara GIOVANELLI*
Digital Ethics Policy Officer

Andy GOLDSTEIN
Legal and Technical Officer

Dirk HOMANN*
Legal Officer

Xanthi KAPSOSIDERI
Legal Officer

Anna LARSSON STATTIN
Legal Officer

Francoise MAYEUR
Supervision and Enforcement Assistant

Adeline MORRIS
Legal Officer

Anne NOEL
Supervision and Enforcement Assistant

Maria Veronica PEREZ ASINARI*
Legal Officer

Lara SMIT
Legal Officer

Snezana SRDIC
Legal Officer

Tereza STRUNCOVA
Legal Officer

Zsofia SZILVASSY
Legal Officer

Kazimierz UJAZDOWSKI
Legal Officer

Jeroen WAUMAN
Legal Officer

Policy and Consultation

Anna BUCHTA
Head of Unit

Olivier MATTER
Head of International cooperation

Chikezie AGUBUZU
Policy & Consultation Assistant

Plamen ANGELOV
Legal Officer/ Seconded National Expert

Sandra BETTI*
Policy and Consultation Assistant

Veronique CIMINA
Legal Officer

Priscilla DE LOCHT
Legal Officer

Claire GAYREL
Legal Officer

Mario GUGLIELMETTI
Legal Officer

Amanda JOYCE
Policy and Consultation Assistant

Laurent LIM*
Legal Officer

Claire- Agnes MARNIER
Legal Officer

Romain ROBERT
Legal Officer

Niksa STOLIC
Legal Officer/ Seconded National Expert

Matthias WILDPANNER- GUGATSCHKA*
Legal Officer/ Seconded National Expert

Agnieszka ZAPOROWICZ
Legal Officer

IT Policy

Thomas ZERDICK
Head of Unit

Massimo ATTORESI
Technology and Security Officer
Data Protection Officer

Dina KAMPOURAKI
Technology and Security Officer

Georgios KOTSAKIS
Technology and Security Officer
LISO

Xabier LAREO
Technology and Security Officer

Frederik LINDHOLM
IT Policy Assistant

Lukasz OLEJNIK
Technology and Security Officer

Robert RIEMANN
Technology and Security Officer

Records Management

Luisa PALLA
Head of Sector

Marta CÓRDOBA HERNÁNDEZ
Administrative Assistant

Kim Thien LÊ
Administrative Assistant

Vincenza MINIELLO
Administrative Assistant

Alison PROCTER
Administrative Assistant

Séverine NUYTEN*
Administrative Assistant

Maria TIGANITAKI
Administrative Assistant

Martine VERMAUT
Administrative Assistant

Information and Communication

Olivier ROSSIGNOL
Head of Sector

Francesco ALBINATI
Information and Communication Officer

Isabelle BARON*
Information and Communication Officer

Thomas HUBERT
Graphic Designer Assistant

Courtenay MITCHELL
Information and Communication Officer

Parminder MUDHAR
Information and Communication Officer

Agnieszka NYKA
Information and Communication Officer

Filippo SEGATO*
Information and Communication Officer

Human Resources, Budget and Administration

Marian SANCHEZ LOPEZ
Head of Unit

Karina REMPESZ
Deputy Head of Unit

Kim BUI
Head of Finance

Cláudia BEATO
HR Assistant

Pascale BEECKMANS
HR Assistant

Laetitia BOUAZZA
HR Assistant
Traineeship Coordinator

Angelo FASSARI
Administrative Assistant

Sebastian GALEA
Finance Assistant

Laurent HAMERS*
Finance Assistant

Sophie JEANNON
Administrative Assistant

Sophie LOUVEAUX
Trainer and Internal Coach

Julia MOLERO MALDONADO*
Finance Assistant

Marco MORESCHINI
HR Officer/ Seconded National Expert
LSO

Anne-Françoise REYNDERS
HR Officer

Jean- Michel VERSTAEN
Finance Assistant

Christophe WALRAVENS*
Procurement & Finance Officer

EDPB Secretariat

Isabelle VEREECKEN
Head of the EDPB Secretariat

Katinka BOJNAR
Legal Officer/ Seconded National Expert

Hannelore DEKEYSER
Legal Officer

Carolina FOGLIA
Legal Officer

Greet GYSEN
Information and Communication Officer

Sarah HANSELAER
Information and Communication Officer

Ahmed IMMOUN
Technology and Security Officer

Joelle JOURET
Legal officer

Zoi KARDASIADOU*
Legal Officer/ Seconded National Expert

Peter KRAUS
Technology and Security Officer
LISO

Fabienne MOLLET
Administrative Assistant

Veronica MORO
Project Officer

Hanna OBERSTELLER*
Legal Officer/ Seconded National Expert

Effrosyni PANAGOU
Assistant of the EDPB Secretariat

Nerea PERIS BRINES
Legal Officer

Andrei PETROVICI*
Technologic and Security Assistant

Aikaterini POULIOU
Legal Officer

Luis SEGURA*
Archivist

João SILVA
Legal Officer
DPO

Constantin STANCU
Archivist

Jasminka TOKALIC
Administrative Assistant

Anne- Marie VANDENBERGHEN
Administrative Assistant

Anna ZAWILA- NIEDZWIECKA
Legal Officer

*staff members who left the EDPS in the course of 2019

Getting in touch with the EU

In person

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

On the phone or by email

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

Finding information about the EU

Online

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

EU publications

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

EU law and related documents

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

Open data from the EU

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

www.edps.europa.eu

@EU_EDPS
EDPS
European Data Protection Supervisor

Publications Office
of the European Union