



EUROPEAN DATA PROTECTION SUPERVISOR



Annual Report

2 0 1 7

. . . .

Executive Summary

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

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

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

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

Luxembourg: Publications Office of the European Union, 2018

© Photos: iStockphoto/EDPS & European Union

© European Union, 2018

Reproduction is authorised provided the source is acknowledged.

Print	ISBN 978-92-9242-253-0	ISSN 1831-0494	doi:10.2804/371265	QT-AB-18-001-EN-C
PDF	ISBN 978-92-9242-252-3	ISSN 1977-8333	doi:10.2804/88867	QT-AB-18-001-EN-N



Annual Report

2 0 1 7

Executive Summary

EUROPEAN DATA PROTECTION SUPERVISOR

| Introduction

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

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

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

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

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

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

With individuals increasingly subjected to varying methods of surveillance, people are beginning to talk about developing a digital ethics, and the EDPS intends to be a leading force in this area. Through the international conference we will host in October 2018, we hope to inspire much-needed debate on this topic across the world and across disciplines, as well as to prepare independent data protection authorities (DPAs) to act as respected guides on the responsible development and application of Artificial Intelligence.

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


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

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

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

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

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



Giovanni Buttarelli
European Data Protection Supervisor



Wojciech Wiewiórowski
Assistant Supervisor

| 2017 - An Overview



@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

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

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

Data protection goes digital

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

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

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

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

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

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

In addition to our work with IPEN, we have also been working hard to develop our knowledge and expertise on new technologies. This knowledge is vital to ensuring that the data protection community is able to respond adequately to new technological challenges

and developments and their implications for data protection and privacy.

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

Data protection does not exist in isolation. It is therefore important that we seek solutions to the challenges of the digital era in collaboration with others. IPEN is a good example of this, as is the Digital Clearinghouse, an EDPS initiative launched in 2016 to facilitate cooperation in the areas of consumer and data protection. Our aim is to work with regulatory bodies to address questions relating to the concentration of market and informational power. The Digital Clearinghouse, which held its first two meetings in 2017, provides a space for dialogue on how to respond to the digital challenge in a way that ensures that individuals maintain control over their personal information.



@EU_EDPS

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

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

Forging global partnerships

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

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

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



@EU_EDPS

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

Our efforts to develop global standards for data protection do not stop at ethics, however. We believe that the EU, when negotiating international agreements, must use these agreements to reinforce the rights of EU citizens, by ensuring that they do not compromise

the levels of data protection provided for under EU law. This is particularly important in the case of trade agreements. Traditionally, data flows have not been considered a trade issue. However, recent calls to include legislation relating to data flows in trade agreements prompted EDPS Giovanni Buttarelli to publish a [blogpost](#) on the subject in December 2017. He repeated the long-standing EDPS position that data protection is not a barrier to international cooperation and that data flows should be kept fully and explicitly out of the scope of the EU's trade agreements.

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

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

Opening a new chapter for data protection

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

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

In the EDPS Strategy, we commit to acting as a proactive partner in discussions between the

European Commission, Parliament and Council on the data protection reform package. We assumed this role throughout discussions on the GDPR, and have adopted a similar approach to ongoing negotiations on the review of [Regulation 45/2001](#), which sets out the rules for data protection in the EU institutions and bodies, and on the reform of the Regulation on ePrivacy.

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

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

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



@EU_EDPS

[#EDPS](#) calls for strong and smart new rules to protect [#confidentiality](#) of communications [#ePrivacy](#)
<https://t.co/rwbDhql4yn>

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

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



@EU_EDPS

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

Meanwhile, in our supervisory role, we took on a new responsibility in 2017: the supervision of Europol. One of our key challenges in this new role is to ensure that Europol is able to strike the right balance between security and privacy when dealing with data processing for the purpose of law enforcement. We have endeavoured to establish effective working relationships with our colleagues at Europol, ending 2017 with a productive inspection of their data processing activities. We look forward to building on these foundations in 2018, and hope that Europol can set an example for others by promoting a mature approach to security and privacy.



@EU_EDPS

#EDPS & JSB handover ceremony set new era in #DataProtection #supervision of @Europol! #EDPS to work as supervisor & advisor

Internal administration

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

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

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

Communicating our message

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

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



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

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

Key Performance Indicators 2017

Key performance indicators (KPIs), established in accordance with the strategic objectives and action

plan defined in the Strategy 2015-2019, help us to monitor the performance of our activities and adjust them, if needed, to increase the impact of our work and the efficiency of our use of resources.

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

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

The following information clarifies the monitoring results of three KPIs:

- KPI 4 analyses the impact of selected EDPS Opinions. This KPI could not be assessed as planned due to delays in the legislative process, which made it impossible to carry out the exercise as planned in relation to the two selected Opinions for 2017 (Directive on digital content and revision of Regulation 45/2001). This KPI is being reconsidered in light of its strong dependence on factors outside EDPS control, such as developments and delays in the legislative process;
- KPI 7 is the composite indicator on visits to the website and Twitter followers. This KPI produced mixed results: while the number of Twitter followers well exceeded the target, the number of visits to the EDPS website was lower than the set target. This is primarily because the figures for 2017 visits to the website only take into account the number of visitors since the launch of the new EDPS website in March 2017. The very positive feedback we received on the new website and the sufficiently high number of visitors allow us to conclude that it remains a valuable online resource for those interested in our work and in data protection in general;
- KPI 8, on staff satisfaction, was not assessed in 2017 as it is linked to the HR survey, a biennial exercise to be carried out again in 2018.

KEY PERFORMANCE INDICATORS		RESULTS AT 31.12.2017	TARGET 2017
Objective 1 - Data Protection goes digital			
KPI 1	Number of initiatives promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	9	9
KPI 2	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8	8
Objective 2 - Forging global partnerships			
KPI 3	Number of cases dealt with at international level (WP29, CoE, OECD, GPEN, International Conferences) for which EDPS has provided a substantial written contribution	31	10
Objective 3 – Opening a new chapter for EU Data Protection			
KPI 4	Analysis of impact of the input of EDPS opinions	<i>N/A for 2017</i>	
KPI 5	Level of satisfaction of DPO's/DPC's/controllers on cooperation with EDPS and guidance, including satisfaction of data subjects as to training	92.3%	60%
KPI 6	Rate of implementation of cases in the EDPS priority list (as regularly updated) in form of informal comments and formal opinions	100%	90%
Enablers – Communication and management of resources			
KPI 7 (composite indicator)	Number of visits to the EDPS website	181 805	2015 as benchmark (195 715 visits to website; 3631 followers on Twitter) +10%
	Number of followers on the EDPS Twitter account	9407	
KPI 8	Level of staff satisfaction	<i>N/A for 2017</i>	

| Main Objectives for 2018

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

Preparing for the EDPB

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

Completing the EU data protection framework

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

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

Preparing for the revised Regulation for the EU institutions

The revised Regulation 45/2001 will define the supervisory role and powers of the EDPS and set out

the rules we must enforce in the EU institutions and bodies. We will therefore continue to devote considerable resources to ensuring the efficient and effective implementation of these rules. This includes updating our internal procedures to bring them in line with the new Regulation and working with the EU institutions and bodies to help them to implement the new rules. Our aim is to ensure that the EU institutions are able to lead by example in their application of the EU's new data protection package.

Effective supervision of Europol

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

Putting our IT expertise into practice

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

Completing the Security Union

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

Guidance on technology and data protection

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

Facilitating the assessment of necessity and proportionality

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

Data protection goes digital

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

We will also work with the [Internet Privacy Engineering Network](#) (IPEN) to raise the profile of privacy engineering. The work of IPEN is vital to ensuring the effective application of data protection by design and by default, bringing together specialists in technology,

law and privacy to promote privacy-friendly technology and privacy-aware engineering techniques. Building on successful workshops with representatives from academia, industry and civil society, IPEN cooperation efforts will intensify in 2018.

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

Moving forward with the Digital Clearinghouse

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

Micro-targeting for non-commercial purposes

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

Integrating ethics into the daily work of data protection authorities

The work of the EDPS and the [Ethics Advisory Group](#) (EAG) over the course of the current mandate has raised the profile of digital ethics in the data protection community. It is now important that we start to integrate ethical insights into our day-to-day work as an independent regulator and policy advisor, and that we cooperate with our colleagues in other [data protection authorities](#) (DPAs) to do so. The [International Conference of Data Protection and Privacy Commissioners](#) (ICDPPC), which will be hosted in Brussels by the EDPS and the Commission for Personal Data Protection of the Republic of Bulgaria

(CPDP) in October 2018, will provide an excellent forum through which to develop and reinforce this cooperation on an international scale.

Preparing for the International Conference

The work of the EAG will conclude in 2018 with the publication of their report, which will provide an

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

| The mid-term Strategic Review

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

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

Evaluating our achievements

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

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

The results of the review allowed us to conclude that there is no need for fundamental changes to the mission or the strategic objectives outlined in the Strategy. All of them remain relevant. There have been no significant, unexpected developments in data protection since the publication of the Strategy in early 2015 and the institution is where we expected it to be at

this point in the mandate. We were also able to predict a number of developments, such as increasing interest in the ethical dimension of the processing of personal data and certain decisions made by the EU Court of Justice (CJEU).

Ensuring an effective approach to the second half of our mandate

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

We also accepted that the workload relating to some tasks, such as Europol Supervision and the setting up of the new European Data Protection Board (EDPB), might have been underestimated. Although our cooperation with stakeholders was generally considered satisfactory, some of those interviewed expressed concerns about future relations with the EDPB and the need for the EDPS to be able to supervise all EU bodies, including those in the areas of Justice and Home Affairs.

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

Both external and internal stakeholders agreed that the organisation is seriously understaffed, both in number and in some fields of expertise. The institution was described as *way too small* to manage its

responsibilities and an ever-increasing workload. The Acting Director will launch a strategic reflection with managers on how to increase resources in the medium-term. We also need to ensure that we take a very selective approach to new challenges, while continuing to train existing staff to help them expand their expertise. The EDPS might also benefit from bringing in advisory bodies with strategic areas of knowledge.

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

The EDPS is in a strong position to influence policies on data protection in Europe. However, even our most optimistic predictions could not have anticipated the

vast increase in interest in data protection from outside European borders. The General Data Protection Regulation (GDPR), which will be fully applicable from May 2018, is now perceived by many as a global standard. Our responsibility for organising the 2018 International Conference of Data Protection and Privacy Commissioners also reflects the EU's position as an international leader in this area. Taking this into account, it might be appropriate to revisit elements of the Strategy to ensure they better reflect the international environment in which we find ourselves.

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

Interview questions

Are there, in your view, any elements that were unknown two or three years ago that would require any changes to the mission or the objectives of the EDPS for the second part of the ongoing mandate (2018-2019)?

Given the transformations and disruptions caused by the current accelerated pace of change, how has the world of data protection evolved in the last three years?

In general terms, has the EDPS been able to transform itself to keep up with these changes? What is your assessment of the role played by the EDPS with the new team of Supervisors?

The world is increasingly dominated by big data, technological game changers, new rules of the game for existing organisations, new entrants and tipping points for the behaviour of the actors: citizens, stakeholders, cyber criminals, terrorists. What are the fundamental challenges both for data protection and privacy as fundamental rights and for the EDPS as an institution in the short- and mid-term? And how is the EDPS equipped for dealing with them? What is it doing well and what needs to change?

In the era of digital transformation and disruption, what is the role of the EDPS in Europe and the world, and how could the EDPS best cooperate with the other players in the field to ensure the carrying out of its vision, mission and goals?

Would you have other suggestions or recommendations for the EDPS?

Additional questions for internal stakeholders:

- How can the EDPS ensure a leading position in the EU and the world?
- What do we need to do to ensure that the EDPS will be one of the big winners in our age of rapid change?



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

