EDPS

European Data Protection Supervisor

ANNUAL REPORT | 2016

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.

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

Freephone number (*)**:**

00 800 6 7 8 9 10 11

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

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

Luxembourg: Publications Office of the European Union, 2017

Print ISBN 978-92-9242-197-7 ISSN 1831-0494 doi:10.2804/66329 QT-AB-17-001-EN-C

PDF ISBN 978-92-9242-202-8 ISSN 1977-8333 doi:10.2804/444401 QT-AB-17-001-EN-N

ANNUAL REPORT | 2016

Executive Summary

EUROPEAN DATA PROTECTION SUPERVISOR

Introduction

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

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

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

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

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

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

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

Our priority will be to make this happen.

Giovanni Buttarelli
European Data Protection Supervisor

Wojciech Wiewiórowski
Assistant Supervisor

2016 - 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

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

Preparing for the changes to come

Much of our work in 2016 focused on preparing for and implementing the GDPR. We worked in close cooperation with our colleagues in the Article 29 Working Party (WP29) to help draft guidance on the new legislation, but also to ensure that we are prepared for the responsibility of both providing the secretariat and acting as an independent member of the new European Data Protection Board (EDPB).

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

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

Moving the global debate forward

As part of our Strategy, we committed to developing an ethical dimension to data protection. In January 2016 we set up the Ethics Advisory Group to examine digital ethics from a variety of academic and practical perspectives. Our aim was to initiate an international debate on the ethical dimension of data protection in the digital era.

@EU_EDPS

@Buttarelli_G #DataEthics Group intends to define new ethical code in the digital environment #CPDP2016

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

The closed session of the 2016 International Conference focused on an equally forward-looking subject: the implications of Artificial Intelligence, machine learning and robotics for data protection and privacy. The EDPS Strategy outlines our dedication to ensuring that data protection goes digital. We therefore sought to inform and steer the debate on this topic

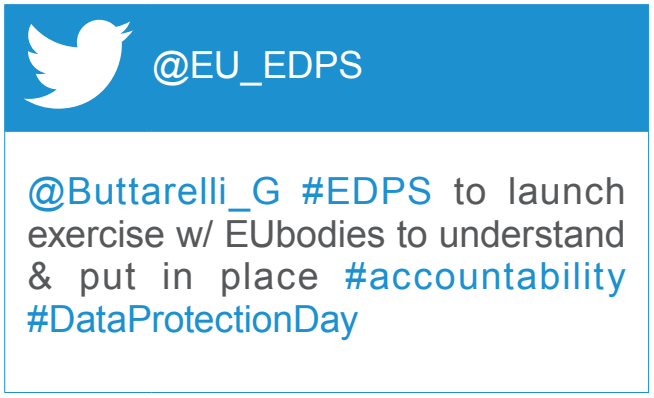
through issuing a very well-received background document for discussion at the conference.

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

EU institutions leading by example

However, achieving our goal of establishing the EU as a leader in data protection on the global stage depends first on the EU institutions setting the standard at European level. As the independent authority responsible for supervising the processing of personal data at this level, we have been actively working with the EU institutions and bodies to help them prepare for the changes to come. Though the GDPR does not apply to their activities, the rules that do will be updated during the course of 2017, to bring them in line with the GDPR.

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



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

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

In recognition of the increasingly important role played by digital communication in the everyday work of the EU institutions, we issued Guidelines on web services and mobile applications in November 2016. The Guidelines offer practical advice on how to integrate data protection principles into the development and management of web-based services and mobile apps respectively, and incorporate input from relevant experts at the EU institutions and bodies, as well as DPOs, ensuring that they remain relevant in practice and not just in theory. We also issued a Guidance document on Information Security Risk Management (ISRM), designed to help those responsible for information security to effectively analyse the data protection risks and determine a set of security measures to be implemented, ensuring both compliance and accountability.

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

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

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

A responsible approach to EU policy

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

Following the 2015 annulment of the Safe Harbour decision by the EU Court of Justice, the Commission negotiated a new adequacy decision with the United States, on which we were consulted in 2016. In our Opinion on the Privacy Shield, which provides for the transfer of data from the EU to the US, we called for a stronger self-certification system, whilst emphasising the need for more robust safeguards on US public authorities' access to personal data, and improved oversight and redress mechanisms.

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

agreement, the transfer of sensitive data in bulk is prohibited.

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

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

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

Internal administration

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

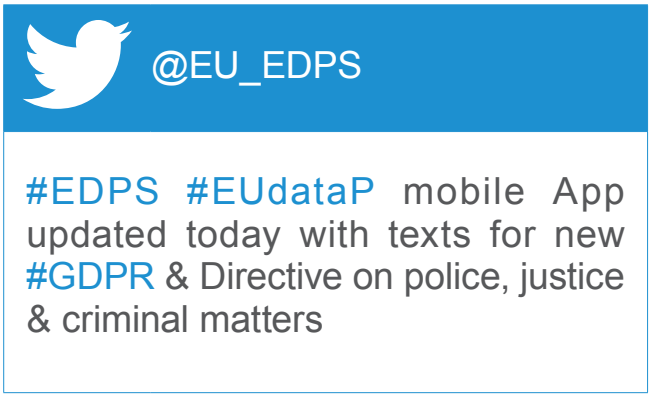
In 2016, staff from the Human Resources, Budget and Administration (HRBA) Unit at the EDPS worked closely with the EDPS DPO to develop and test our accountability tool. We also implemented internal policies, such as an ethics framework, aimed at increasing transparency and promoting professionalism.

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

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

Communicating our message

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



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

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

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

Key Performance Indicators 2016

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

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

The KPI scoreboard contains a brief description of each KPI, the results on 31 December 2016 and the set target. The indicators are measured against initial targets in most cases, but there are two KPIs that have been calculated for the first time: KPI 5 and KPI 9.

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

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

Main Objectives for 2017

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

Ensuring confidentiality and privacy in electronic communications

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

Preparing for the revised Regulation 45/2001

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

Facilitating the assessment of necessity and proportionality

In 2016 we published a background paper on necessity and launched a stakeholder consultation. Taking into account the feedback received, in early 2017 the EDPS will publish a necessity toolkit. It will provide guidance to EU policymakers and legislators responsible for preparing measures which involve the processing of personal data and which interfere with the right to the protection of personal data. We will follow up with a background document on the principle of proportionality in EU data protection law and will organise workshops devoted to specific EU policy areas, in order to train Commission staff and raise their awareness of data protection issues.

Promoting stronger borders based on respect for fundamental rights

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

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

Preparing the EU institutions for Data Protection Impact Assessments

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

Guidance on technology and data protection

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

Revising EDPS Guidelines on health data

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

The Spring Survey

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

Developing our expertise in IT security

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

International cooperation

Continued cooperation with national DPAs will be essential in 2017. In addition to continuing our joint preparations for the GDPR, we will work with the WP29 on subjects including the security agenda and new counter-terrorism measures, international transfers, financial data, health and IT developments. We will also work with DPAs in our role as a European data protection secretariat, not only for the EDPB but also in our work on coordinated supervision of large-scale IT systems and the supervision of Europol.

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

Accountability project

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

Developing an ethical dimension to data protection

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

Monitoring technology

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

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

Data protection goes digital

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

Preparing for the EDPB

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

Effective supervision of Europol

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

Setting up the Digital Clearing House

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

Awarding those who apply privacy enhancing technologies

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

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

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

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

Priced publications:

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

www.edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Superviser

EDPS
European Data Protection Supervisor

Publications Office