EUROPEAN DATA PROTECTION SUPERVISOR

ANNUAL REPORT | 2015

An Executive Summary of this Report which gives an overview of key developments in EDPS activities in 2015 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.

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, 2016

Print	ISBN 978-92-9242-092-5	ISSN 1830-5474	doi:10.2804/27186	QT-AA-16-001-EN-C
PDF	ISBN 978-92-9242-090-1	ISSN 1830-9585	doi:10.2804/641327	QT-AA-16-001-EN-N
EPUB	ISBN 978-92-9242-091-8	ISSN 1830-9585	doi:10.2804/5606	QT-AA-16-001-EN-E

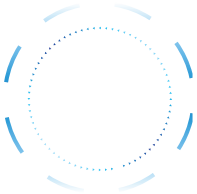
© European Union, 2016

© Photos: iStockphoto/EDPS & European Union

Reproduction is authorised provided the source is acknowledged.

Printed in Italy

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)



ANNUAL REPORT | 2015

European Data Protection Supervisor

Contents

► **FOREWORD** 5

► **MISSION STATEMENT, VALUES AND PRINCIPLES** 7

► **EDPS STRATEGY 2015-2019** 8

1. 2015 - An Overview 9

1.1 Data protection and the EDPS in 2015 9

1.2 Data protection reform 9

1.3 Leading by example 10

1.4 Data protection on the ground 10

1.5 Cooperation with data protection authorities in the EU 10

1.6 Identifying policy solutions 11

1.7 Technology 11

1.8 International interaction 12

1.9 Communicating our message 12

1.10 Internal administration 12

1.11 Key Performance Indicators 2015-2019 13

2. 2015 Highlights 14

2.1 Borders 14
2.1.1 Bordering on privacy: Frontex launches PeDRA 15
2.1.2 EDPS warns against unjustified and massive collection of passenger data 15
2.1.3 Biometric border control 16
2.1.4 Effective supervision of large-scale IT systems 16

2.2 Security 18
2.2.1 Keeping eCommunications privacy friendly 18
2.2.2 IT security 18

2.3 Responding to new challenges 21
2.3.1 Towards a new digital ethics 21
2.3.2 New technologies 22
2.3.3 Big data 23
2.3.4 Competition 23
2.3.5 Health data 24
2.3.6 Police and justice 25
2.3.7 Legislative reform 25

2.4 Global dimension **26**
2.4.1 International transfers in the post-Safe Harbour world 26
2.4.2 Increased tax transparency, decreased data protection 27
2.4.3 Keeping track of TTIP 27
2.4.4 International enforcement cooperation 27
2.4.5 Cooperation with the Council of Europe 27
2.4.6 Developing digital security at the OECD 28
2.4.7 Working with the WP29 28
2.4.8 Tackling technological challenges with the IWGDPT 28
2.4.9 International conferences 29
2.4.10 Coordinated Supervision of large-scale IT systems 29

2.5 On the ground **30**
2.5.1 Employment 30
2.5.2 Whistleblowing 31
2.5.3 Fraud 32
2.5.4 Cloud computing 32
2.5.5 Financial data 33
2.5.6 DPO Network 34

3. Court Cases 35

4. Transparency and Access to Documents 38

5. The Secretariat 39

5.1 Information and communication **39**
5.1.1 Online media 39
5.1.2 New visual identity 40
5.1.3 Events and publications 40
5.1.4 External relations 41

5.2 Administration, budget and staff **42**
5.2.1 Budget and finance 42
5.2.2 Human resources 43
5.2.3 European Data Protection Board (EDPB) 44
5.2.4 A competition for data protection specialists 44

6. The Data Protection Officer at the EDPS 45

6.1 The DPO at the EDPS **45**

6.2 Leading by example **45**

6.3 Advising the institution and improving the level of protection **45**

6.4 The register of processing operations **45**

6.5 Providing information and raising awareness **45**

7. Main Objectives for 2016 46

Annex A - Legal framework 49

Annex B - Extract from Regulation (EC) No 45/2001 51

Annex C - Supervision and Enforcement activities 53

Annex D - List of Data Protection Officers 57

Annex E - List of prior check and non-prior check opinions 59

Annex F - List of Opinions and formal comments on legislative proposals 62

Annex G - Speeches by the Supervisor and Assistant Supervisor in 2015 63

Annex H - Composition of EDPS Secretariat 67

Foreword

2015 will be remembered as the year the EU seized an historic opportunity. The General Data Protection Regulation (GDPR) is one of the EU's greatest achievements in recent years. It is a set of data protection rules for the digital age, an ambitious and forward-thinking agreement of which the EU can be proud.

The exponential rise in the amount of personal data generated, analysed and monetised with minimal human intervention or knowledge has put major strains on the data protection principles enshrined in the Charter of Fundamental Rights of the EU. It was therefore essential to update and reinforce the foundations and structure of data protection law.

In our Strategy 2015-2019 we outlined our intention to open a new chapter on data protection, through adopting and implementing up-to-date data protection rules. In the first year of our mandate we have been fully engaged in encouraging and advising the Parliament, Council and Commission in this endeavour, providing article-by-article recommendations on the texts of the GDPR. We did so in the form of an app - an unprecedented exercise in digital transparency, used by negotiators as a reference guide.

However, agreement on the GDPR is only the first step in the modernisation process. Our focus now turns to its implementation. This will involve ensuring the accountability of controllers, increasing cooperation with independent data protection authorities (DPAs) and empowering their activities through the establishment of the European Data Protection Board (EDPB) and effectively responding to the *Schrems* judgment by implementing sustainable rules on data transfers. The principles of the GDPR also need to be fully integrated into a modernised framework for the privacy of all electronic communications, with the review of Directive 2002/58/EC.

We have also taken steps to actively confront the challenges of technological change, through the launch of an Ethics Advisory Group. The Group will consider the ramifications of data-driven technologies for human dignity and freedom. Their work will take place in full public view and will be debated in an international forum in 2017. We are confident that this project will have a lasting and positive impact.

In 2015, we also invested new energy in our core tasks as a supervisor. The 2015 Survey of data protection officers in EU institutions and bodies demonstrates that they are now better equipped than ever to lead by example in the responsible processing of personal data.

Finally we would like to express our gratitude to our members of staff. This first year of our mandate has been very demanding, and we pay tribute to the energy, creativity and commitment of our colleagues, which has enabled this first year to be so successful. With their support, the EDPS will remain a bold and unapologetic champion of EU values, with a global vision for sustainable data processing. This includes strengthening cooperation with privacy regulators and with global partners, but also building new partnerships, as we continue to ensure that the EU leads by example in the global dialogue on data protection and privacy in the digital age.

Giovanni Buttarelli
European Data Protection Supervisor

Wojciech Wiewiórowski
Assistant Supervisor

Mission statement, values and principles

The European Data Protection Supervisor is the European Union's independent data protection authority established under Regulation (EC) No. 45/2001, devoted to protecting personal information and privacy and promoting good practice in the EU institutions and bodies.

- We **monitor** and **ensure** the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals.
- We **advise** EU institutions and bodies on all matters relating to the processing of personal information. We are consulted by the EU legislator on proposals for legislation and new policy developments that may affect privacy.
- We **monitor** new technology that may affect the protection of personal information.
- We **intervene** before the EU Court of Justice to provide expert advice on interpreting data protection law.
- We **cooperate** with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information.

We are guided by the following values and principles in how we approach our tasks and how we work with our stakeholders:

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 policy and 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 impact on privacy. We act selectively and proportionately.

EDPS Strategy 2015-2019

The EDPS Strategy 2015-2019 was adopted on 2 March 2015. It aims to provide a framework through which to promote a new culture of data protection in the European institutions.

About the Strategy

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

This 2015-2019 Plan summarises:

- the major data protection and privacy challenges over the coming years;
- three strategic objectives and 10 accompanying actions for meeting those challenges;
- how to deliver the strategy, through effective resource management, clear communication and evaluation of our performance.

Our aims and ambitions build on our strengths, successes and lessons learned from implementing our *Strategy 2013-2014: Towards Excellence in Data Protection*.

Vision, Objectives and Action 2015-2019

The EDPS' vision is to help the EU lead by example in the global dialogue on data protection and privacy in the digital age. Our three strategic objectives and 10 actions are:

1 Data protection goes digital

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

(2) Identifying cross-disciplinary policy solutions;

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

2 Forging global partnerships

(4) Developing an ethical dimension to data protection;

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

(6) Mainstreaming data protection into international policies.

3 Opening a new chapter for EU data protection

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

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

(9) Facilitating responsible and informed policymaking;

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

@EU_EDPS

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

1. 2015 - An Overview

1.1 DATA PROTECTION AND THE EDPS IN 2015

In March 2015 we launched our Strategy 2015-2019, *Leading by Example*. Our aim was to seize the historic opportunity to develop data protection over the period of our new mandate. The Strategy sets out our objectives for the coming five years and the actions necessary to achieve them. The Key Performance Indicators (KPIs) outlined in this report have been developed to ensure that we are fully accountable and transparent on how we achieve our objectives.

First and foremost we outlined our commitment to open a new chapter for European data protection through supporting the negotiation and adoption of innovative and future-oriented data protection rules. We provided the EU legislators with detailed recommendations on the proposed data protection reform and made them widely available in a user-friendly mobile app, which allowed users to compare the proposed texts from the Commission, the Parliament and the Council alongside the EDPS recommendations. This required a huge effort but it made the legislative process more transparent for the public and the legislators themselves. It has ensured that the three legislative bodies and their data protection authority can be held accountable for their contributions to the process. In December 2015, final agreement on the General Data Protection Regulation (GDPR) was reached. This hugely significant reform undoubtedly marks one of the EU's greatest achievements in recent years.

Second, we stressed the role of the EU institutions themselves in setting the standard and leading by example in implementing the reform. Over the course of 2015 we worked closely with Data Protection Officers (DPOs), carried out detailed inspections and provided the EU institutions with support and advice, notably in the form of the Guidelines on eCommunications and mobile devices. As the data protection authority of the EU institutions and bodies we will continue to support them in preparing for the changes to come over the course of 2016.

At the international level the EDPS was at the forefront of both the EU and the global debate on privacy and data protection throughout 2015. There are now 109 countries which have data protection laws in place, and many look to the EU as an example. As an ambassador for EU data protection, in 2015 the EDPS both visited and welcomed visits from data protection authorities around the world. We increased our contribution at international level through our continued participation in international fora and cooperation with international organisations, as well as through new initiatives, such as the preparations for an Ethics Advisory Group.

As technology continues to develop and to transform our lives it is essential that data protection *goes digital*. We have to promote technological solutions which both support innovation and enhance privacy and data protection, in particular by increasing transparency, user control and accountability in big data processing. Our work in 2015 put the EDPS at the centre of these discussions. Our Opinions on big data, mobile health (mHealth), and intrusive surveillance all called for specific actions to maximise the benefits of new technology without compromising the fundamental rights to data protection and privacy.

Our mandate and our Strategy are designed to address the current period of unprecedented change and political importance for data protection and privacy, both in the EU and globally, and the EDPS intends to ensure that the EU remains at the forefront of the debate. Our Strategy of leading by example will be pursued further in 2016, as we look to build on the achievements of 2015 and develop innovative solutions to the data protection challenges which face us.

1.2 DATA PROTECTION REFORM

After almost four years of intense negotiation and public debate, political agreement on the General Data Protection Regulation was reached in December 2015. The EDPS was active as an advisor throughout this process, including meeting with civil society organisations in May.

Our final message to the legislators was in July, when we provided them with our first set of comprehensive, article-by-article recommendations for enhancing safeguards, cutting bureaucracy and ensuring the relevance of the reform during the next generation of technological change. We launched this Opinion in the form of a free-to-download mobile app, which allowed users to compare the Commission proposal, the Parliament and Council texts for negotiation and the EDPS recommendations, all on one screen.

In October, we added our detailed recommendations on the proposed Directive for the sectors of police and

justice to this app, urging the legislators to be consistent in the standards required of all controllers, with only limited deviations to account for the special circumstances of law enforcement data processing.

Our focus in 2016 will turn to advising the legislators on the completion of the reform, firstly through the effective implementation and application of these principles to EU institutions and bodies, through the reform of Regulation 45/2001, and secondly, to the confidentiality of all communications, with the reform of the ePrivacy Directive.

1.3 LEADING BY EXAMPLE

In September we called for a new digital ethics; one which puts human dignity at the heart of personal, data-driven technological development. This Opinion provided the basis for our discussions with companies, regulators and academics in the US (in San Francisco and Silicon Valley) that same month, and at the International Conference in Amsterdam in October. It also announced our intention to set up an Ethics Advisory Group, to be appointed in January 2016, which will look into the longer term implications of big data, the internet of things and artificial intelligence.

Additionally, in 2015 we initiated a project to develop a framework for greater accountability in data processing. This was applied first of all to the EDPS, as an institution, a manager of people and financial resources and a controller, informing our development of internal rules, as well as institution-wide guidance on whistleblowing and a code of conduct for the Supervisors.

In the course of 2015, we also organised two meetings with Data Protection Officers (DPOs) in which we discussed topics such as accountability, IT security and data protection impact assessments. We also involved DPOs in the preparation of our contribution to the reform of Regulation 45/2001. Throughout the year we issued 70 Opinions on notifications of processing operations, many on recruitment and staff appraisal, and dealt with 143 complaints, 30% more than in 2014. We visited five EU agencies, in addition to conducting our bi-annual compliance survey, the results of which will be published in January 2016.

1.4 DATA PROTECTION ON THE GROUND

In 2015, we undertook five important inspections. These included an inspection of recruitment activities at the European Commission's Directorate General for Human Resources (DG HR) and an inspection at the European Investment Bank (EIB), concerning its handling of sensitive data in fraud investigations and anti-harassment procedures. We also issued two Opinions on data processing as part of due diligence controls for combating money-laundering and terrorism financing at the European Investment Fund (EIF).

Through carrying out inspections and responding to consultations and notifications, we ensure that the EU's large-scale IT systems –Eurodac (for processing asylum requests), Visa Information System (VIS), Schengen Information System (SIS), Customs Information System (CIS) and the Internal Market Information System (IMI)- comply with data protection rules. In 2015, we inspected SIS and VIS. We also issued an Opinion on plans by the EU Agency for the Operational Management of Large-scale IT systems in the area of freedom, security and justice (eu-LISA) to consider the use of Multi-Spectrum Imaging devices to scan fingerprints as part of the asylum procedure and the storage of this data in a database maintained by the agency. In 2016 we will urge the EU institutions and bodies to consolidate existing platforms for the law enforcement sector in the interest of more coherent and effective supervisory arrangements.

In 2015 we dealt with five requests under the 2001 Public Access to Documents Regulation. Two important rulings by the EU Court of Justice in 2015 also helped to clarify the relationship between transparency and data protection. In *Dennekamp v. European Parliament*, the Court held that uncovering conflicts of interest was sufficient justification for granting access to information about MEPs affiliated to a now defunct pension scheme. In *ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA)*, the Court held that transparency regarding the identity of external experts involved in an EFSA guidance document was necessary to demonstrate their impartiality and ensure accountability. The EDPS intervened in both cases.

In its judgment on 3 December, the Court also followed our legal reasoning on the question of the information to be provided to a petitioner when requesting consent for the publication of his personal data, which included sensitive health data.

1.5 COOPERATION WITH DATA PROTECTION AUTHORITIES IN THE EU

We have continued to be an active member of the Article 29 Working Party (WP29), focusing our efforts where we can add most value. This has included work on the Opinion on applicable law, on the Commission's proposed Data Protection Code of Conduct for Cloud

Service Providers and liaison with the Council of Europe's Cybercrime Committee. At the annual Spring Conference we encouraged our partner authorities to speak with one authoritative voice to present credible solutions for global digital challenges.

In cooperation with the WP29, for budgetary reasons we began a preliminary analysis of logistical arrangements for providing the Secretariat for the European Data Protection Board (EDPB), which will come into force with the new data protection reform. In close liaison with the WP29 we have set up an internal task force which will facilitate the transition, so that the Secretariat and the Board can be fully operational from day one. We are also contributing to another preparatory task force, established with national colleagues at the last WP29 plenary meeting of 2015.

Similarly, we have been preparing for the expansion of our coordinated supervision role, which will likely encompass Europol, Smart Borders, Eurojust and the European Public Prosecutor's Office.

Separate from our supervision responsibilities, we have continued to serve as secretariat to the supervision coordination groups for CIS, EURODAC, VIS, SIS II and the IMI. We aim to support the launch of a new website as a resource for these groups in 2016.

1.6 IDENTIFYING POLICY SOLUTIONS

The vigorous debate on big data has continued following the publication of our Opinion on the subject. In addition to numerous speaking engagements, in September 2015 we hosted *Competition Rebooted* in collaboration with the Academy of European Law, a workshop aimed at deepening understanding in this area. We announced that a second Opinion on competition would be published in 2016 and, over the next year, we intend to encourage a Europe-wide dialogue among regulators, academics, industry, the IT community and consumer protection organisations on big data, the internet of things and on fundamental rights in the public and private sectors.

We also advised the institutions on new legislation, such as the proposed EU Passenger Name Record (PNR) Directive. This Directive would potentially allow for the collection of personal data from all airline passengers in the EU. In September 2015 we issued an Opinion on PNR, highlighting the lack of evidence to justify such a sweeping measure.

We have closely followed developments on the Transatlantic Trade and Investment Partnership (TTIP). EDPS Giovanni Buttarelli delivered a speech before the European Parliament calling on the EU to ensure that TTIP, as well as any other new agreement, fully respects EU data protection standards.

The management of the EU's external borders in the face of unprecedented migration flows was perhaps one of the biggest political concerns for the EU in 2015. Border management involves processing the personal information of millions of individuals.

During 2015 we provided advice to Frontex, the EU border agency, on the *PeDRA* project, which aims to enable the agency to act as a hub for information collected by Member States on suspected smugglers or traffickers. We were involved at several stages in the development of this project and issued a prior checking Opinion in July, to ensure data quality and security and to prevent discriminatory profiling.

The EDPS has also been working with the European Medicines Agency (EMA) on the anonymisation of clinical reports for the purpose of publication. In our first policy Opinion of the new mandate we tackled the opportunities and risks of mobile health apps and services, and provided recommendations on how to build trust through transparency, user control and data protection safeguards.

In our July Opinion on the EU-Switzerland agreement on the automatic exchange of tax information, we aimed to set down principles in an area of proliferating international accords in the OECD campaign against banking secrecy in tax matters. We have also provided advice to the Commission and the European Central Bank (ECB) on the reform of securities markets, the prevention of market abuse and collection of detailed credit information.

In 2016 we will continue to develop a comprehensive toolkit which will enable EU bodies to take informed decisions on data protection, depending on where the need is greatest.

1.7 TECHNOLOGY

With data security a growing concern for all organisations, in 2015 we issued Guidelines on the use of electronic communications and mobile devices in the workplace. We also worked with EU institutions and their Data Protection Officers (DPOs) to ensure the implementation of effective security measures, such as encryption, and participated in an inter-institutional project for encrypting emails. Guidelines on web services, mobile apps and cloud computing will be

concluded in 2016, complemented by guidance on specific areas such as accountability in IT management and risk management.

Through our Newsletters and our Opinions on big data and mobile health we have continued to monitor and report on the data protection implications of new technologies. Meanwhile, the Internet Privacy Engineering Network (IPEN) has continued to grow, focusing its work on standardisation initiatives on privacy, online tracking and privacy engineering.

As cloud computing will soon become the standard way of computing, we increased our engagement with legislators, the industry and the EU institutions and bodies in 2015, focusing on how to exploit the potential of this technology whilst also remaining in control of personal data. We encouraged EU institutions and bodies to establish a common IT strategy, and supported the first inter-institutional Call for Tender for the provision of cloud-based services- Cloud I.

The Hacking Team affair revealed the capabilities of software for infiltrating IT systems and covert surveillance. In our December Opinion on the subject we therefore called for more monitoring and regulation of the market for spyware, especially with the growth of the internet of things.

We will continue to develop our expertise in the area of IT security throughout 2016 and, through our inspection and auditing activities, ensure that the relevant rules are applied. This includes acting as a partner to all members of the IT security community, with a particular focus on the EU institutions and bodies.

1.8 INTERNATIONAL INTERACTION

In 2015 we continued to promote international standards for data protection and enforcement cooperation among data protection authorities (DPAs).

The preliminary ruling of the EU Court of Justice (CJEU) in October declared the EU-US Safe Harbour decision invalid. With our partners in the Article 29 Working Party (WP29), we called on the EU and the US to put in place a more sustainable legal instrument which respects the independence of DPAs. We also worked with Data Protection Officers (DPOs) to draw up a map of transfers taking place in the EU institutions and bodies under the Safe Harbour scheme.

Data protection reform is also on the agenda of the Council of Europe, and in 2015 we continued to contribute to the work of the committees responsible for modernising Convention 108. We have also been involved in the OECD's Working Party on Security and Privacy in the Digital Economy, preparing proposals for a risk-based approach to data protection, to be discussed at the ministerial conference on the digital economy in Cancun in June 2016.

We continued to deepen our engagement with APEC, GPEN, the French-speaking association of personal data protection authorities (AFAPDP), the Ibero-American data protection network, the Berlin Group and the international conference of data protection and privacy commissioners and will look to keep expanding our international partnerships in 2016.

1.9 COMMUNICATING OUR MESSAGE

In May, we launched a new EDPS logo. At the end of the year we completed the first phase of updates to the EDPS website. These projects mark a new era for the EDPS and for data protection.

There was a dramatic increase in engagement with our social media platforms, especially on Twitter where both our followers and number of tweets increased significantly, but also on LinkedIn and YouTube, for which we increased our efforts.

In addition to three editions of the EDPS newsletter, we issued 13 press releases and answered 31 written media enquiries, while the EDPS and Assistant EDPS gave 39 direct interviews to European and international journalists. Our heightened visibility was reflected in the appearance of the EDPS in over 400 articles, radio broadcasts, videos or other media in 2015.

Our outreach activities also expanded in 2015. We welcomed a record number of visitors to our stand at the annual EU Open Day on 9 May and organised seven study visits for groups from European universities and youth organisations. In addition to the open meeting with civil society on data protection reform, both the Supervisors and EDPS staff are increasingly active as ambassadors of the EU approach to privacy, as was evident in our sponsorship of the annual Computers, Privacy & Data Protection conference.

1.10 INTERNAL ADMINISTRATION

Amid the challenges of a new mandate and the changing data protection landscape, we have pursued ambitious goals with a small team of dynamic, talented and highly motivated EU officials.

In 2015 we received a clean report from the Court of Auditors for the fourth consecutive year and have

continued to improve the implementation rate of our budget. We established new policies on learning and development, career guidance and equal opportunities and, with EPSO, held a specialist competition for data protection experts. This resulted in a reserve list of 21 exceptional candidates which will cover the forthcoming recruitment needs of the EDPS and the future EDPB.

In 2015, the EDPS was allocated a budget of EUR 8 760 417, an increase of 1.09% compared to the 2014 budget. We improved the implementation of our budget to around 94% in 2015, compared with 85% in 2011, whilst also complying with Commission austerity guidelines and budget consolidation. We also met twice with the finance team of the European Ombudsman in 2015 to identify common needs, as a basis for closer collaboration in 2016.

1.11 KEY PERFORMANCE INDICATORS 2015-2019

Further to the adoption of the Strategy 2015-2019, in March 2015, the existing key performance indicators (KPIs) were re-evaluated to take into account the objectives and priorities of the new Strategy. As a result, a new set of KPIs were established, to help us to monitor and adjust, if needed, the impact of our work and the efficiency of our use of resources.

The table here shows the performance of our activities in 2015 in accordance with the strategic objectives and action plan defined in the Strategy 2015-2019.

The KPI scoreboard contains a brief description of each KPI, the results on 31 December 2015 and the target set.

In most cases, the indicators are measured against initial targets. For three indicators, the results of 2015 will be used as a benchmark. Two KPIs will be calculated starting in 2016. The results show that the implementation of the Strategy is largely on track and no corrective measures are needed at this stage.

One key performance indicator (KPI 7) did not meet the initial target. This was mainly due to changes in planning at the European Commission, which resulted in initiatives being postponed until 2016. Additionally, on one occasion the EDPS was not consulted by the Commission.

KEY PERFORMANCE INDICATORS		RESULTS AT 31.12.2015	TARGET 2015
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	2015 as benchmark
KPI 2	Number of activities focused on cross-disciplinary policy solutions (internal & external)	9	8
Objective 2 - Forging global partnerships			
KPI 3	Number of initiatives taken regarding international agreements	3	2015 as benchmark
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	13	13
Objective 3 - Opening a new chapter for EU Data Protection			
KPI 5	Analysis of impact of the input of EDPS to the GDPR		To be calculated starting 2016
KPI 6	Level of satisfaction of DPOs/DPCs/controllers on cooperation with EDPS and guidance, including satisfaction of data subjects as to training	79.5%	60%
KPI 7	Rate of implementation of cases in the EDPS priority list (as regularly updated) in form of informal comments and formal opinions	83%	90%
Enablers - Communication and management of recources			
KPI 8 (composite idicator)	Number of visits to the EDPS website Number of followers on the EDPS Twitter account	195 715 3631	2015 as benchmark 2015 as benchmark
KPI 9	Level of Staff satisfaction		To be calculated starting 2016

2. 2015 Highlights

The EDPS is responsible for ensuring that the European institutions and bodies respect fundamental rights when processing personal data and developing new policies. We have three main fields of work:

- **Supervision:** This involves monitoring the processing of personal data in the EU administration and ensuring compliance with data protection rules. Our tasks range from prior checking processing operations likely to present specific risks, to handling complaints and conducting enquiries.

- **Consultation:** Our consultation work involves advising the European Commission, the European Parliament and the Council on proposals for new legislation and on other issues which impact on data protection.

- **Cooperation:** We cooperate with national data protection authorities (DPAs) to promote consistent data protection throughout Europe. Our main platform for cooperation with national DPAs in the EU is the Article 29 Working Party (WP29).

Our work in these fields centres on the five main themes covered in the 2015 Annual Report.

As terrorism and migration rated high on the EU agenda in 2015, our work on borders has taken on increasing importance. The EDPS ensured that data protection and privacy remain primary concerns, both by providing advice on new legislation to combat terrorism and by continuing to effectively supervise the large-scale IT systems used by the EU to process visa, asylum and other similar requests.

With continued developments in technology, our work on security, particularly as it relates to the day-to-day work of the EU institutions and bodies, remained a strong focus for the EDPS. During 2015 we issued Guidelines on the use of electronic communications and mobile devices in the workplace, whilst also working with EU institutions and bodies and their Data Protection Officers (DPOs) to ensure the implementation of effective security measures such as encryption.

2015 presented many new challenges and much of our work focused on how to respond to them. We monitored new technologies, releasing Opinions on big data and mobile health and worked with other EU institutions and bodies to address the data protection concerns raised by a number of EU initiatives. We also launched two new projects, the Ethics Advisory Board and our mobile app on the General Data Protection Regulation (GDPR), both aimed at promoting a proactive approach to data protection in the EU and globally.

In accordance with the vision outlined in our Strategy 2015-2019, in 2015 we worked hard to develop the global dimension of our work. We contributed fully to European and international fora and actively monitored and provided advice on international agreements with an impact on data protection.

We also worked with EU institutions and bodies *on the ground*. Throughout 2015 we supervised and provided advice to the EU institutions, carrying out inspections, issuing prior check Opinions and developing our relationships with the DPOs who are responsible for ensuring compliance with data protection law within their respective EU institutions.

Finally within the Secretariat we made significant improvements to our communication tools and methods, increased our administrative and financial efficiency, and took several initiatives to improve the working conditions of our staff (see Chapter 5).

2.1 BORDERS

The main purpose of EU border security is to safeguard European values and interests, including our fundamental rights, the rule of law and freedom of movement.

Managing our borders is therefore far more complicated than simply checking passports. In fact, Member States use a variety of systems to control their borders, all of which involve collecting large amounts of personal data.

Even before reaching the border, personal data from nationals in need of an EU visa will be registered in the EU's Visa Information System (VIS). Asylum seekers are enrolled in Eurodac to check for multiple asylum applications made by the same person. Individuals barred from entering the Schengen zone are registered in the Schengen Information System (SIS), as are those for whom a European Arrest Warrant has been issued. These databases and others, managed at European

level and used by designated authorities in the Member States, and in some cases by Europol, contain personal information about a vast number of people.

The EDPS plays an important role in ensuring that these various databases and exchange tools are used in a way that complies with data protection rules. This involves acting both as a supervisor, carrying out inspections and responding to consultations and notifications, and as an advisor, issuing Comments on proposals for new legislation and providing guidance, through workshops and other activities. Our work in 2015 has focused on the concepts of necessity and proportionality, ensuring that the amount of data collected in relation to EU border activities does not exceed that which is truly necessary.

At the end of 2015, the Commission issued a legislative proposal for transforming Frontex, the EU's border agency, into a European Border and Coast Guard. They also announced a new smart borders package. Border management will therefore continue to be an important aspect of EDPS work in 2016.

@EU_EDPS

#necessity not only #proportionality is by law daily routine for all DPAs including EDPS

2.1.1 Bordering on privacy: Frontex launches PeDRA

Irregular migrants stopped at Europe's borders and victims of human trafficking can often provide valuable information about their smugglers or traffickers. However, this information is collected on a national level and may not reach other competent authorities which might be able to investigate these cases further.

To help solve this problem, the EU's border agency, Frontex, is currently developing a pilot test under the name of *personal data in risk analysis* (PeDRA). Through PeDRA, Frontex could act as a hub for organising, processing and identifying connections between the information gathered by individual Member States. Though the agency is forbidden from processing the personal data of victims, it can process the data of suspected smugglers or traffickers and transfer any relevant information to Europol.

However, there are concerns which the project must address in order to be compliant with data protection rules. These include how to prevent discriminatory profiling, how to make sure that the information received is reliable and how to ensure that such sensitive data is kept safe.

Taking this into account, Frontex notified the EDPS of this project when it was in its early stages of development. We provided input at several junctures, most importantly in our prior checking Opinion of 3 July 2015. Frontex is making good progress in implementing our recommendations and has announced it will start a pilot test of the project in early 2016.

2.1.2 EDPS warns against unjustified and massive collection of passenger data

On 25 September 2015, the EDPS issued its second Opinion on the EU Passenger Name Record (PNR) Directive. The original proposal was rejected by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) in April 2013 but was reintroduced for discussion in February 2015, following the terrorist attacks in France.

The Directive provides for the default collection of massive amounts of personal information from millions of travellers. While we fully recognised the need to combat the terrorist threat, we found that none of the available information on the issue demonstrated a real need to collect large amounts of passenger data for this purpose.

The proposed EU PNR scheme could cover all flights to and from the EU, and possibly also intra-EU and domestic flights. This would entail the collection of personal data from more than 300 million passengers. We encouraged the legislators to demonstrate that

collecting this data is both necessary and proportional to the achievement of their aims and to look for alternative solutions, such as new investigative approaches and more selective surveillance measures. We also stressed the importance of analysing the impact of the proposed measures on the fundamental rights of individuals to the protection of personal data and privacy.

Trilogue discussions between the Commission, Parliament and Council took place at the end of 2015 to agree on the final text of the Directive, which is likely to be adopted in 2016.

@EU_EDPS

#EDPS supports EU legislator on #security but recommends re-thinking on #EUPNR

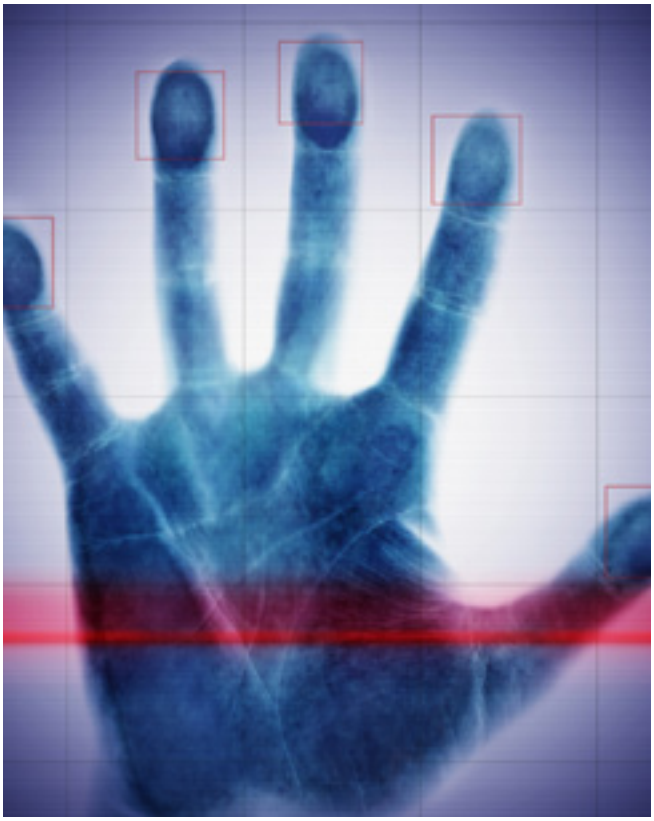
2.1.3 Biometric border control

On 28 January 2015, eu-LISA, the EU Agency for the Operational Management of Large-scale IT systems in the area of freedom, security and justice, informed the EDPS of an assessment they planned to carry out on the performance of Multi-Spectrum Imaging (MSI) devices, for the scanning of fingerprints. The assessment aimed to determine if these devices could be used in Eurodac, a fingerprint database used to assist the asylum procedure.

The assessment involved testing the MSI devices with real fingerprints, provided by the competent national authorities of the Member States of the European Economic Area (EEA). The national authorities would collect, store and transfer this biometric data to a dedicated database maintained by eu-LISA.

The EDPS issued an Opinion on the data protection implications of this project on 25 November 2015. As the first step of this process will take place at national level, and is therefore covered by national data protection law, our recommendations focused on the collection and storage of fingerprints by eu-LISA.

We advised the agency to provide adequate information to the public about the use of this data. This might be done by publishing a specific privacy statement on their website. We also advised them to take adequate measures to ensure the security of the biometric data involved.

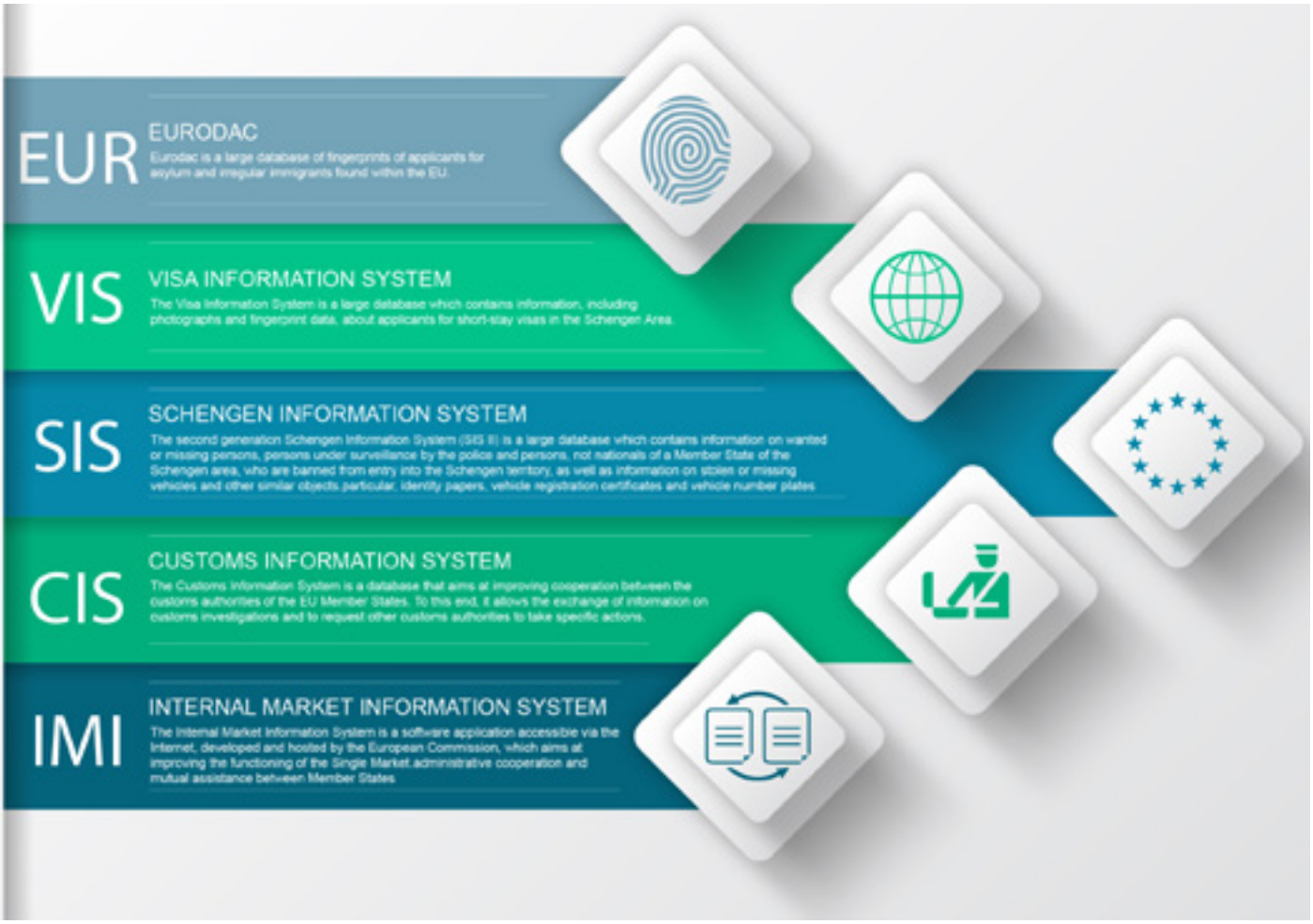


2.1.4 Effective supervision of large-scale IT systems

In order to increase cooperation and information exchange between national authorities and, in some cases, EU bodies, a number of European large-scale IT systems have been created.

Most of these systems consist of a national unit, supervised by the relevant national data protection authorities (DPAs), and a central unit. The central units of the following five systems are supervised by the EDPS:

- Eurodac (the European fingerprint database for identifying asylum seekers)
- Visa Information System (VIS)
- Schengen Information System (SIS)
- Customs Information System (CIS)
- Internal Market Information System (IMI)



Some of these systems include vast amounts of data. For example, Eurodac contains the fingerprints of more than two million individuals while the VIS tracks tens of millions of visa applications. To guarantee the rights of those registered in these systems, consistency between the activities of the different supervisory authorities is essential. It is therefore important that the EDPS and national DPAs work together to fully coordinate our supervision activities and ensure consistency.

Inspections: VIS and SIS pass the data protection test

Inspections are a tool used by the EDPS to monitor the application of data protection rules in the EU institutions and bodies and ensure that personal data is used correctly. We provide inspected institutions with detailed feedback on how they can improve their compliance with data protection rules.

In 2015, in line with SIS and VIS regulations, the EDPS launched two inspections to check the security and operational management of these databases, which are used by border guards, customs officers, and visa and law-enforcement authorities throughout the Schengen area. As these systems handle so much personal data and are accessible to a range of users, it is essential to determine that they are being managed in a way that complies with data protection law.

The SIS inspection report was finished in 2015 and shared with the Council, the European Parliament, the Commission, national authorities and eu-LISA, the EU agency responsible for managing these systems. The VIS report will be finished and distributed accordingly in 2016. We will follow-up on our recommendations to ensure that both systems remain fully compliant with data protection rules.

Subgroup continues to keep the Schengen system safe

The technical expert subgroup of the Schengen Information System II Supervision Coordination Group (SIS II SCG) was created in 2013. Composed of security experts from both the EDPS and DPAs from

the Member States, the group deals with technical security topics related to SIS.

Our work in 2015 focused on two items: the development of a security audit framework, designed to ensure consistency in the performance of inspections; and the development of a roadmap to deal with data breaches, should SIS II ever be affected. We were also able to visit eu-LISA, the EU agency responsible for the management of SIS, to get a better knowledge of its capabilities and interact with their technical staff.

The security audit framework will help to ensure that inspections cover all possible security concerns, by providing straightforward guidance on the specific elements that must be assessed. The collection of inspection data using the framework (or the relevant parts of the framework) will make analysis of the results much easier, as well as drafting the inspection report and recommendations. In future when inspections are carried out using the same framework, we will be able to compare results across time and across the different parts of SIS. This is a valuable tool that will both ensure the consistency of the supervisory activities of the EDPS and DPAs and ensure effective compliance.

The subgroup also started working on a roadmap for how to respond if SIS II was to fall victim to a data breach. As the SIS II legal framework does not contain specific rules on how to respond in the event of a personal data breach, it is necessary to define a coherent process to deal with this possibility. Much of the groundwork for this project was completed in 2015. We will continue working with the Data Protection Officer (DPO) at eu-LISA in 2016 to produce the final roadmap.

2.2 SECURITY

2.2.1 Keeping eCommunications privacy friendly

On 16 December 2015, the EDPS published Guidelines for the EU institutions and bodies on personal data and electronic communications (eCommunications). These Guidelines offer practical advice on how to integrate data protection principles into the management of email, internet and telephony for work purposes.

Organisations using eCommunications process the personal information of their employees, for instance, in the management of eCommunication services, billing and verifying authorised use. Furthermore, as it is often permitted to use work equipment for private communication, interference by an employer with the use of eCommunications by employees is therefore likely to touch upon private information.

The Guidelines highlight the general data protection principles that will help EU institutions and bodies comply with the Data Protection Regulation. They also include easy-to-use checklists in order to facilitate the day-to-day work of controllers. While they are addressed to the EU institutions and bodies, the Guidelines might also be useful for a wider audience. This is because the Data Protection Regulation applicable to the EU institutions and bodies is similar in many respects to the Data Protection Directive which is implemented into the national laws of EU Member States.

The Guidelines build on the extensive practical experience we have gained through our supervision work, on previous EDPS decisions and Opinions (on administrative consultations, prior checks and complaints), and on the work of the Article 29 Working Party. Although they are based on the current data protection legal framework, they are designed to remain relevant when the new framework comes into force as they focus on the accountability of organisations to demonstrate that they are complying with their data protection obligations.

2.2.2 IT security

Data protection goes mobile

On 16 December 2015, the EDPS published Guidelines on the protection of personal data on mobile devices used by EU institutions and bodies. Aimed principally at Data Protection Officers (DPOs), as well as IT and IT security staff, the Guidelines provide practical advice concerning the processing of personal data via mobile devices.

The EDPS Strategy 2015-2019 outlines the importance of increasing the accountability of European institutions processing personal information. In practice this means helping them not only comply with EU data protection rules but to be able to clearly demonstrate their compliance. To ensure that our Guidelines support them in this, we engaged in a structured and open dialogue with the EU institutions and bodies, asking for their comments on both the content and format of the Guidelines, with a view to providing a practical document which can be readily applied in the workplace.

Mobile devices, such as phones, tablets, laptops and netbooks allow staff to work remotely. These devices present common risks due to their portability and small size. The measures to mitigate these risks, therefore, such as security access to office networks, need to be specifically tailored. The Guidelines are designed to help EU institutions and bodies to do this.

Once again, while these Guidelines are aimed at EU bodies, anyone or any organisation interested in data protection and mobile devices might find them useful since they are based on the common EU data protection principles currently implemented in the national laws of EU Member States.

Ensuring website security

In 2014 we reported on our efforts to improve the security of the EDPS website through encryption. We built on this experience in 2015 to address user complaints about the lack of adequate security provided on the webpages of some of the other EU institutions.

We advised the EU institutions concerned that, when personal information is exchanged online, it is necessary to secure this data with adequate encryption. This minimises the risk of eavesdropping and of unauthorised modification of data submitted online, which is possible when data is transferred through insecure communication infrastructures, such as unencrypted Wi-Fi hotspots.

Our recommendations on this topic will be compiled in a comprehensive set of Guidelines on the web services of the EU institutions and bodies, to be finalised in 2016.

Encryption: Security threat or protector of privacy?

Terrorist attacks in Europe and the ongoing discussion on government surveillance have prompted some calls for restrictions on encryption, ways to break it or the weakening of encryption tools for consumers.

The risks of such an approach for the economy and society at large are significant and have already been analysed and discussed many times in the past; the integrity of encryption has been recognised as necessary for the digital economy and for the protection of fundamental rights, such as privacy and free speech. The Council of Europe, the European Parliament and the European Commission have all defended the right to and need for encryption to protect personal data.

The EDPS followed this discussion closely throughout 2015 and the use of encryption for economic and social purposes was the subject of Assistant Supervisor Wojciech Wiewiórowski's presentation at the Free and Safe in Cyberspace Conference, in Brussels on 24-25 of September 2015.

Encryption makes bulk data collection and mass surveillance difficult, but it also preserves our fundamental rights to data protection and privacy, through providing a secure means of communication. It is also not a limiting factor in more targeted and specific security measures. Law enforcement requires the means to fight crime on the internet, but it is important to ensure that any new measure is both necessary and proportional to this aim.

@EU_EDPS

Fundamental role of #cybersecurity in ensuring protection of individuals' rights to privacy online #cspforum

EDPS participates in Encrypted Electronic Communications project

The EU institutions and bodies have a duty to protect the personal information they use and exchange in order to safeguard the privacy of individuals or the interests of the European Union. The EDPS is participating in an inter-institutional pilot project on Encrypted Electronic Communications in the European institutions, which aims to ensure that this duty is respected.

Coordinated by the European Commission, the project aims to support the implementation of secure electronic communications within the European institutions by applying state-of-the-art encryption technology to the email services of the institutions. In the long-term, this solution will be interoperable with EU citizens and businesses.

To achieve these aims, the project will:

- document the business needs of the EU institutions and bodies;
- provide a complete overview of existing solutions related to secure communication across the EU institutions and identify and assess other possible solutions, and;
- recommend an approach for both a short- and long-term solution, which assesses its feasibility, identifies the prerequisites, proposes a deployment plan and identifies the roles and responsibilities of each institution or body as well as procedures to ensure end-to-end security.

The project will conclude in 2016.

Dealing with data breaches

Data breaches have become increasingly high profile in recent months and represent a direct threat to the security of personal data. It therefore constituted an important topic of discussion at the first of our twice-yearly meetings with the Data Protection Officers (DPOs) of the EU institutions and bodies on 8 May 2015.

We addressed the topic from the perspective of risk management, taking into account the variety of possible security threats, vulnerabilities, and events that could occur in the case of a data breach. We stressed the need for each EU institution to set up an appropriate Information Security Risk Management process, to ensure that they are prepared should they ever have to deal with a data breach.

Shortly after the meeting, on 22 May 2015, the EDPS was notified of a security and data breach at an EU institution. We welcomed the fact that the institution contacted the EDPS, provided information to those affected, and implemented a well-organised incident management plan.

Technical error leads to data protection breach

In spring 2014, a technical error led one European institution to publish personal information about its staff on its website. The information, which had been collected for internal purposes and was meant for publication on the institution's internal network, included job descriptions, first names and, in some cases, photos. One member of staff complained about this breach, which the EDPS investigated.

We concluded that a breach of Article 22 of the Data Protection Regulation had occurred in this case. However, we also concluded that the institution responded to the breach in a satisfactory manner and had taken the necessary measures to prevent a similar breach from recurring in the future.

EDPS issues alert on intrusive surveillance

Hacking Team is an Italian company which sold highly sophisticated software capable of gaining access to computers all over the world. In July 2015, they were the victim of an attack that resulted in the publication of all their internal emails, sales details, sold software and technical documentation. The leaked documents showed that this intrusion software was sold to several EU and non-EU governments. More importantly, however, the leaked documents described in detail the capabilities of the tools sold and used by government and law enforcement authorities to investigate the electronic lives of individuals.

A component of these tools actively infiltrates IT systems by using vulnerabilities in commonly used platforms and software. Once the system is infiltrated, the intrusion software installs and activates its surveillance functions which allow it to bypass encryption, collecting data out of any device and monitoring a target covertly and remotely.

@EU_EDPS

Aim of #surveillance measures must be #legitimate and the means #proportionate #EUdataP

On 15 December 2015, the EDPS published an Opinion on intrusive surveillance technology. We highlighted the risks posed by the unregulated and growing market for the sale, distribution and (dual) use of spyware and emphasised that more needs to be done to monitor the market. We called on legislators to look for safeguards which embed privacy by design in technology and ensure that it is secure.

Surveillance tools can be instruments for legitimate and regulated use by law enforcement bodies. However, they can also be used to circumvent security measures in electronic communications and data processing, thereby undermining the integrity of databases, systems and networks. As the internet of things becomes more widespread, so the risks will become more significant.

We called for a coordinated approach to tackle these risks, including better regulation of the trade and use of surveillance software in the private sector, to ensure that the privacy of all individuals in the EU is protected both at home and abroad.

2.3 RESPONDING TO NEW CHALLENGES

2.3.1 Towards a new digital ethics

On 11 September 2015 we issued an Opinion on new digital ethics. We urged the EU and those responsible internationally to promote an ethical dimension in future technologies in order to retain the value of human dignity and prevent individuals from being reduced to mere data subjects.

The Opinion also announced our intention to set up an external ethics advisory group that would help to better assess the ethical implications of how personal information is defined and used in the big data and artificial intelligence driven world. This announcement built on the commitment we outlined in the EDPS Strategy 2015-2019 to launch such a group to explore the relationships between human rights, technology, markets and business models in the twenty-first century.

@EU_EDPS

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

In 2015 we carried out the preparations necessary to allow the group to start work in early 2016. In late 2015 we issued a call for expressions of interest which was published on the web and in print media. On the basis of the responses received, we started the process of selecting eminent and independent personalities to become members of the group. The selection process will be completed by the end of January 2016 and the group will start work shortly after.

2.3.2 New technologies

Effective data protection requires advanced security and risk management. It is therefore vital to keep track of new technological developments to ensure that all risks are assessed and appropriate security measures are implemented.

As well as monitoring major technological advances such as the internet of things and big data analytics, we also examined less prominent technological changes. Many of these have been the subject of dedicated EDPS initiatives, such as the use of mobile apps, the use of mobile devices, cloud computing, smart grids, intelligent transport and surveillance and investigation tools.

Other areas we have been monitoring include online tracking technologies, particularly those used in relation to targeted advertising and the emergence of new technological solutions for tracking the location of individuals. We work closely with our colleagues at other data protection authorities (DPAs) to assess these technologies and provide advice to controllers and citizens.

Smart policies for smart technologies

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

In 2012, the Commission issued recommendations on the security and protection of personal data in this process. They created a template for carrying out a Data Protection Impact Assessment (DPIA) and identified Best Available Techniques (BATs), a list of products available on the market that could be used to protect personal data. The Article 29 Working Party, to which the EDPS belongs, was involved as an advisor in this project.

In October 2014, the DPIA Template began a 2-year test phase, which carried on throughout 2015. Criteria to assess the BATs were also established in 2015.

The EDPS will continue to support this project, which could be used as the basis for work on other smart technologies.

Engineering privacy: IPEN continues to grow

The Internet Privacy Engineering Network (IPEN), which was launched in 2014, has continued to grow.

The initiative has gained many new members from industry, academia and civil society and has begun to develop strong support structures to better facilitate cooperation between its members.

The network was presented at several conferences in 2015, including CPDP 2015, the Annual Privacy Forum and ISSE 2015. A dedicated IPEN workshop was also held in cooperation with the Belgian data protection authority and with the support of the Catholic University of Leuven. The workshop covered topics such as standardisation initiatives on privacy, the findings of recent investigations in online tracking and educational initiatives on privacy engineering.

IPEN members also closely followed negotiations on the General Data Protection Regulation (GDPR). Many provisions in the reform will create considerable challenges for IPEN as we look to translate these obligations into data protection friendly engineering requirements and methods.

Intelligent data protection for Intelligent Transport Systems

In November 2014, the European Commission launched its platform for cooperative intelligent transport systems (C ITS).

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

Privacy considerations are very important in the deployment of C ITS as the technology used can collect huge amounts of data, including location, vehicle model and identification number, speed or acceleration and the personal information of C ITS users, all of which could be used for profiling or tracking people.

The EDPS continued to follow this initiative throughout 2015. Specifically, we called attention to the possible challenges of safeguarding data quality and security and of facilitating accountability and purpose limitation. We also highlighted the need to ensure that the principle of transparency and the fundamental right to data protection were upheld. We recommended that particular attention be given to facilitating privacy by design, defining roles and responsibilities, identifying security concerns and informing users about the collection, storage and usage of their personal data.

2.3.3 Big data

Meeting the challenges of big data

The internet has evolved in such a way that the tracking of people's behaviour has become an essential source of revenue for some of the world's most successful companies. A critical assessment of the situation is needed and a search for workable alternatives.

In our Opinion of 19 November 2015, we outlined this need to launch a new, open discussion with legislators, regulators, industry, IT experts, academics and civil society to explore how the social benefits of big data can be harnessed while protecting the dignity and fundamental rights and freedoms of individuals in a more effective and innovative way.

We called upon organisations to be accountable and transparent, to develop a new ethical approach to how they handle the personal data they collect, and in this way foster consumer trust as part of a smart business strategy. Greater user control over their data will help to ensure that individuals are able to better detect unfair biases and challenge mistakes. It will also mean that individuals are given a genuine and informed choice about how their data is used.

@EU_EDPS

#BigData getting bigger = big responsibility to guard our rights more closely. Need to debate how to balance the two

Open data meets data protection

On 1 June 2015, the Joint Research Centre (JRC) of the European Commission wrote to the EDPS about a research project which involved testing a series of functionalities and algorithms, such as gender and age determination, on a publicly available research dataset of images containing people. The aim was to help develop techniques to fight online child abuse.

In our response of 3 December 2015, we advised the JRC that they should only process the personal data necessary for the research project and that they should explain to the individuals whose pictures and metadata were collected, in a clear and comprehensive privacy notice, why their personal data was being used. We specified that the re-use of the dataset proposed would only be permitted as long as the processing of the data was not likely to cause any damage or distress to those concerned. Lastly, we informed the JRC that no personal data should be published in the results of the research, only the data concerning the performance results of the algorithm and a reference to the dataset.

2.3.4 Competition

Keeping competition data protection friendly

In 2014, the EDPS published an Opinion on big data and competitiveness. It focused on the relationship between personal data protection, competition law and consumer law, based on the notion that while personal data may enhance the economic performance of market players in many industries, it might also have an impact on *consumer welfare*.

We followed this Opinion in September 2015 with *Competition Rebooted*, a one-day workshop on data protection and competition hosted in collaboration with the Academy of European Law (ERA). The purpose of the workshop was to explore if and how personal data processing impacts the market, in light of new

technologies and business models, and what the policy response should be. The workshop was attended by data protection practitioners, scholars and competition experts and several cases and topics were discussed.

Following the workshop, we began thinking about preparations for a second Opinion on the topic, an idea which we will develop in 2016.

2.3.5 Health data

Ensuring anonymity

In 2015 the EDPS and the European Medicines Agency (EMA) held several high level meetings on the anonymisation of clinical reports for the purpose of publication. The relevant data protection legislation clearly states that *no personal data shall be publicly accessible*. Given that all data relating to an identifiable individual must be considered personal, the preparation of clinical data for publication poses particular challenges.

In their meetings with the EMA, both the EDPS, Giovanni Buttarelli, and the EDPS Director, Christopher Docksey, discussed future-oriented solutions to ensure the strong and robust anonymisation of personal data in the publication of clinical reports, stressing the need to uphold data protection principles.

Healthcare on the move

Mobile technology is revolutionising the healthcare market, offering opportunities to benefit the global population with a variety of healthcare needs. The convergence between technology and healthcare is expected to allow patients access to better healthcare at a lower cost, improved control over their own healthcare and easier and more immediate access to medical care and information online.

Big data is impacting mobile health (mHealth) in a big way. The potential to collect a huge amount of personal information (physiological, preferences, emotions and so on) and to buy, sell and analyse it without the full knowledge and consent of the individuals concerned has to be addressed by industry and governments - and by us, as consumers of these technologies.

In our Opinion, published on 21 May 2015, we stressed the need to make transparent the ways and purposes for which personal data is processed, shared and re-used, for instance through easy-to-read privacy policies which are highlighted rather than hidden away and a list from which you can actively choose to opt-in or out.

@EU_EDPS

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

Failure to deploy data protection safeguards would result in a critical loss of individual trust, leading to fewer opportunities for public authorities and businesses, hampering the development of the health market. To foster confidence, future policies need to encourage service providers and their associates to be more accountable and place respect for the choices of individuals at their core. They must also end the indiscriminate collection of personal information and any possible discriminatory profiling, encourage privacy by design and privacy settings by default and enhance the security of the technologies used.

More people are taking a proactive role in checking or monitoring their health than ever before. The enhanced power of ubiquitous new computing devices is helping to drive this growth, but individuals should not only be empowered to be proactive over health, they should be empowered over their personal lives as a whole. Transparency, awareness and effective control over personal information all contribute to such empowerment. We need solutions on how to stay connected on the move that also respect our privacy and personal identity.

2.3.6 Police and justice

New supervisory role for the EDPS

In 2015 the EDPS continued to provide advice to the legislators on specific data protection issues related to the new Europol Regulation, which was agreed upon in December 2015 and is expected to come into force in spring 2017. Under the new Regulation, the EDPS will become the supervisor of Europol with regard to the processing of personal data, taking over the majority of the functions currently performed by the Joint Supervisory Body of Europol.

A Cooperation Board will also be put in place to allow closer cooperation with the national supervisory authorities of the Member States. It will work as an advisory body on matters involving the processing of personal data by Europol which originate in the Member States. The Board will meet when necessary and at least twice a year, with the EDPS providing its Secretariat.

Progress has also been made on the new regulations for Eurojust and the European Public Prosecutor's Office (EPPO). A draft General Approach to the Eurojust Regulation was concluded in March, while plans relating to the proposed structure and organisation of the EPPO are still in the negotiation phase.

2.3.7 Legislative reform

GDPR: EDPS recommendations for reform

After almost four years of negotiation, the General Data Protection Regulation (GDPR) was agreed upon in December 2015. The GDPR will replace the current Directive 95/46/EC.

Ever since the European Commission presented the original legislative proposal in January 2012, the Reform has been the subject of intense debate. The EDPS followed developments throughout the legislative process, providing advice to the EU co-legislators (the European Parliament and the Council) at various stages.

On 27 July 2015, we produced our recommendations on the proposed legislation, for use by the EU co-legislators when negotiating the final text of the GDPR. We also launched a mobile app, allowing tablets and smartphones to be used to easily compare the texts proposed by the Commission, the European Parliament and the Council, alongside the recommendations from the EDPS.

The proposed new rules will affect all individuals in the EU, all organisations in the EU who process personal data and organisations outside the EU who offer goods or services to the EU or monitor the behaviour of individuals in the EU. It represents an opportunity for Europe to lead by example on a global level, setting the standard for the rest of the world to follow.

@EU_EDPS

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

Recommendations for reform in the police and justice sectors

The GDPR will only apply to activities in the private sector. A separate Directive has been proposed by the Commission to cover the sectors of police and justice.

On 28 October 2015 the EDPS published an Opinion on the proposed Directive for the sectors of police and justice, followed by a mobile app allowing users to compare the proposed texts of the Commission, Parliament and Council, once again alongside the recommendations from the EDPS.

In our Opinion, we reaffirmed that data protection in the police and justice sectors should remain consistent with the general rules contained in the GDPR, and that adjustments should only be introduced where necessary, in view of the specific nature of these sectors.

We called on the legislators to ensure that the Directive continued to uphold the level of protection currently offered by EU law and the Council of Europe. We also emphasised that the essential components of data protection law, laid down in Article 8 of the Charter of the Fundamental Rights of the Union, must be respected, with any exceptions strictly limited, and be able to fulfil the strict test of proportionality. We also specified that, where necessary, existing agreements concluded by the EU or Member States involving the transfer of personal data should be amended within a fixed time limit, to bring them in line with the new Directive.

In our examination of the outcome of the trilogue, which ended in December 2015, we noted that, among other things, several specific safeguards for data protection were either maintained or introduced in the final text. This included the distinctions to be made between different categories of data subjects, and the distinction between personal data based on facts and personal data based on personal assessments.

2.4 GLOBAL DIMENSION

In a hyper-connected world with evolving technologies and increasing exchanges of personal information, the protection of personal data requires a coordinated and cross-border approach. The EDPS monitors technological developments and their impact on the protection of personal data, but we also advise EU institutions and bodies on the protection of personal data when they negotiate international agreements or take positions in international fora.

Throughout 2015, we provided input on relevant documents discussed in international institutions and organisations. We also attended meetings and participated as members or observers in negotiations on relevant legislation.

Moreover, we tried to monitor and provide advice on data protection developments in non-EU countries and on privacy policies in international organisations (such as UNHCR), with the aim of ensuring that these countries or organisations, as potential recipients of EU data, provide the highest level of data protection possible.

We work hard to ensure that the construction of an international system of enforcement cooperation among data protection authorities, potentially including the exchange of personal data, respects EU and international data protection principles.

2.4.1 International transfers in the post-Safe Harbour world

On 6 October 2015, the Court of Justice of the European Union (CJEU) declared the European Commission's Safe Harbour decision invalid. It argued that, due to the threat of US mass surveillance, personal data transferred to the US under the arrangement was not adequately protected.

In response to the ruling, we worked with our colleagues in the Article 29 Working Party (WP29) to analyse the consequences of what is now known as the *Schrems* decision. We also contributed to the various subgroups in charge of evaluating the consequences of the decision, for example, examining its impact on alternative ways of transferring data to the US, such as BCRs and contractual model clauses and on US legislation regarding access to data by public authorities, and working together with all national data protection authorities (DPAs) to deal with any issue regarding the actions to be taken in cases involving the transfer of data to the US.

We informed Data Protection Officers (DPOs) in all EU institutions and bodies of the Court's judgment and on 23 October 2015 we launched a data mapping survey, asking DPOs to report any transfers taking place under the Safe Harbour scheme within their respective institutions. The EDPS will continue working on the results of this survey to gain a better understanding of which EU institutions and bodies were most dependent on the Safe Harbour scheme. This will help to determine the actions to be taken by the EDPS after the WP29 publishes its Opinion on EU-US data transfers at the beginning of February 2016.

Over the course of 2015, we received one complaint and a request for consultation by an individual regarding transfers by EU institutions and bodies to recipients in the US carried out under the Safe Harbour scheme, and opened investigations on these cases.

2.4.2 Increased tax transparency, decreased data protection

On 8 July 2015, the EDPS published an Opinion on the EU-Switzerland agreement on the automatic exchange of tax information. The Opinion came in response to the EU's adoption, on 27 May 2015, of an amending protocol to the Savings Agreement, an agreement between the European Community and the Swiss Confederation in the area of tax cooperation.

The new agreement builds on earlier bilateral agreements with Switzerland, Andorra, Liechtenstein, Monaco and San Marino. It aims to regulate the exchange of financial, tax-relevant information between governments in the EU and Switzerland, putting an end to banking secrecy in tax matters. It will harmonise EU relations with Switzerland in line with EU and international developments in this area, through the use of the *automatic exchange of information*.

However, though the agreement represents an important step in the fight against tax evasion, the data protection provisions included in the agreement do not go far enough. We therefore called on the Commission to ensure that adequate data protection safeguards are implemented in similar bilateral agreements dealing with automatic exchange of tax information in the future.

In our Opinion, we outlined five specific recommendations which should be taken into account when negotiating future bilateral agreements in this area and which should be introduced in any updated versions of agreements that have already been finalised. These recommendations include making the collection and exchange of tax-relevant information conditional on the risk of tax evasion, only processing data in pursuit of a legitimate policy goal and specifying an explicit retention period for the tax information exchanged.

2.4.3 Keeping track of TTIP

Throughout 2015, we followed discussions between the EU and the US on the Transatlantic Trade and Investment Partnership (TTIP). We kept in close contact with the Commission and the European Parliament to ensure that data protection remained out of the scope of the agreement and would not impact the high standard of data protection provided for in EU law. We will continue with this approach up until the conclusion of the agreement.

2.4.4 International enforcement cooperation

Throughout 2015, we have provided input on discussions in the Council of Europe (Consultative Committees of Convention 108 and the Cybercrime Convention), the OECD, APEC, GPEN, the French-speaking association of personal data protection authorities (AFAPDP), the Ibero-American data protection network, the Berlin Group and the international conference of data protection and privacy commissioners.

We have monitored and contributed to the discussions of the Council of Europe Committee on the Cybercrime Convention and have sought to avoid the addition of any binding protocol on direct access by law enforcement authorities to data stored in third countries, as this would contradict the EU and Council of Europe data protection frameworks.

2.4.5 Cooperation with the Council of Europe

The Council of Europe is an important player in privacy and data protection law and policy, not only in Europe but increasingly on other continents where pan-European norms are often taken as a source of inspiration for legislation and policies. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (*Convention 108*) is open to accession by both European and non-European countries. It is used as a tool to help spread the European model of data protection as a fundamental and human right. The Council of Europe also encourages cooperation between its member states in other areas such as law enforcement, where privacy and data protection aspects must be taken into account.

The EDPS is an observer in the Council of Europe's expert groups on data protection, including the Consultative Committee (T-PD) of Convention 108 and the ad hoc committee on data protection (CAHDATA), entrusted with the modernisation of Convention 108. In 2015 we attended the meetings of these expert groups and provided informal oral and written comments and recommendations. We will continue to engage in negotiations on the modernisation of Convention 108 to ensure a good level of protection is achieved and that the text is compatible with the outcome of the EU data protection reform.

We also attended meetings of the Cybercrime Committee (T-CY), including the Cybercrime@Octopus Conference, held from 17-19 June 2015, to ensure that data protection considerations are taken into account in their work.

2.4.6 Developing digital security at the OECD

The EDPS participates at staff level in the OECD's *Working Party on Security and Privacy in the Digital Economy*. The main objective of this group is to support the development of digital security and privacy from a risk analysis perspective.

Privacy is often considered alongside security, rather than as an independent concept. This means that many data protection considerations, as well as the fundamental rights perspective, are often overlooked. Additionally, risk analysis can be challenging in a privacy context as the risk is different depending on whether it is assessed from the point of view of the individual or the company.

Specific issues we have raised in this group include their view of interoperability in trans-border data flows, the limits of a harm-based approach to privacy, and the difference between privacy and security.

The group is currently focused on preparation for the ministerial conference on the digital economy which will take place in Cancun in June 2016. The papers being prepared for the conference are in line with the risk-based approach advocated by the EDPS, as is the group's 2016 work programme.

2.4.7 Working with the WP29

The Article 29 Working Party (WP29) is made up of representatives from the national data protection authorities (DPAs) of each EU Member State and the EDPS. As our advisory role coincides to some extent with the role of the WP29, we aim to ensure effective coordination with our partner supervisory authorities.

As a member of the WP29, we actively contribute to the Group's activities, taking up a share of the work, within the various subgroups, comparable to that of the other DPAs. Our participation is based on a selective approach, ensuring that our work focuses on the areas in which our contribution provides the most added-value. This usually relates to our ability to provide an EU perspective, such as in the Working Party Opinion on applicable law, or in the response to the cybercrime committee of the Council of Europe on the impact of data protection regarding the Budapest Convention.

Additionally, we cooperate with the WP29 in preparations for the future European Data Protection Board (EDPB), for which the EDPS will provide the Secretariat.

2.4.8 Tackling technological challenges with the IWGDPT

The International Working Group on Data Protection in Telecommunications serves as an early warning mechanism to alert privacy and data protection authorities globally about new technological challenges for personal data protection. Also known as the Berlin Group, as it is facilitated by the Berlin Commissioner for Data Protection and Information Freedom, it is composed of data protection and privacy commissioners, including the EDPS, from Europe, America, Asia-Pacific and Africa, and a limited number of invited legal and technical experts from civil society, academia and business. Its task is to provide its members and the public with working papers on specific technological developments.

@EU_EDPS

#technology serves man not the other way round @Buttarelli_G #EUdataP

2.4.9 International conferences

Leading by example at the European conference

Data protection authorities (DPAs) from EU and Council of Europe member states meet annually at the European Conference of Data Protection Authorities. The conference is an opportunity to discuss matters of common interest and exchange information and experience on different topics.

The UK's Information Commissioner's Office (ICO) hosted the most recent conference, which took place in Manchester from 18-20 May 2015. It focused on the topics of cooperation, data subject rights and the roles and responsibilities of data protection authorities and controllers.

EDPS Giovanni Buttarelli used the conference as an opportunity to update European colleagues on the work and priorities of the EDPS. Speaking at the conference, he focused on the goals outlined in the EDPS Strategy 2015-2019 and stressed the importance of cooperation and *active partnership* between the EDPS and its fellow DPAs. With specific reference to the data protection reform, he emphasised that speaking with one voice on EU data protection is the best way to ensure that the opinions of EU DPAs are heard at legislative level.

He also stressed the importance of DPAs leading by example when handling personal information and performing supervisory duties. In doing so, the decisions and opinions of DPAs will gain more weight and credibility, allowing us to increase our influence, both within the EU and globally.

Two resolutions were adopted at the conference, the first on meeting data protection expectations in the digital future and the second on the opening of a dedicated European Conference section on the European Commission's CIRCABC platform.

Elaborating on ethics at the International conference

The annual International Conference of Data Protection and Privacy Commissioners took place in Amsterdam from 26-29 October 2015. Hosted by the Dutch data protection authority, the Conference was an opportunity for data protection leaders from across the world to discuss some of the most important issues in data protection and privacy today.

The main theme of the conference was privacy bridges. Discussion on this topic focused on a report prepared by a group of EU and US experts in privacy and data protection. The report identifies ten practical steps, or bridges, that will result in better-informed, and more consistent, regulatory cooperation, policy guidance, and enforcement activity across the world, without any change in the law.

Also discussed were the privacy challenges of genetic data. Due to technological developments, it is likely that genetic data will soon be widely available. As the genetic information of one individual also contains information about their ancestors and descendants, it is essential that we begin to address the personal data protection implications of developments in genetic analysis.

Side events at the conference were an opportunity to exchange ideas on the role of ethics in data protection. Following the announcement that the EDPS intended to appoint an external Ethics Advisory Group in early 2016 (see section 2.3.1), EDPS Giovanni Buttarelli and Assistant Supervisor Wojciech Wiewiórowski participated in a discussion on this topic, where they were able to elaborate and gain feedback on their plans.

Giovanni Buttarelli also participated in the final high level panel of the conference, which focused on the future of data protection. The discussion proved particularly interesting given the recent decision of the Court of Justice of the European Union to suspend the Safe Harbour agreement between the US and the EU.

The international conference adopted four resolutions, on transparency reporting, humanitarian action, the UN special rapporteur on the right to privacy and the strategic priorities of the conference.

2.4.10 Coordinated Supervision of large-scale IT systems

The European Union has set up a number of European large-scale IT systems serving different purposes in various areas (see section 2.1.4). As these systems include vast amounts of data, a coordinated approach

is necessary in order to ensure a high level of data protection. Supervision of these systems is therefore shared between the national data protection authorities (DPAs) and the EDPS, who meet regularly in distinct groups dedicated to each individual system.

The EDPS is in charge of providing the Secretariat of the supervision coordination groups of CIS, EURODAC, VIS, SIS II and the IMI. This work is additional to and separate from our supervision work in those areas (see section 2.1.4) and our role as a member of each group. In 2015, we organised two meetings for each of the coordinated supervision groups. We ensure that the meetings of all groups take place one after the other so that consistent and horizontal supervision policies are implemented where possible. We also draft and circulate relevant documents for group discussions and liaise with the Chairs and members of the groups to prepare the meetings, ensure follow-up and continue work on ongoing exercises in between meetings.

The coordinated supervision model may develop in future years as the Commission has proposed similar models in a number of legislative initiatives, such as those on Europol, Smart Borders, Eurojust and the European Public Prosecutor's Office (EPPO).

2.5 ON THE GROUND

2.5.1 Employment

Commission demonstrates data protection compliance

In early 2015, we inspected the Directorate General for Human Resources (DG HR) at the European Commission. This inspection was significant as DG HR is a large organisation, responsible for processing personal information related to selection and recruitment within the DG and also for advising other Commission DGs on how to integrate data protection principles into their recruitment activities.

Our inspection, therefore, focused on the selection procedures used by DG HR, specifically on how personal information is handled, the right of individuals to access their data and the physical, electronic and organisational security of this data.

We checked that the personal information processed in recruitment activities can be considered as relevant and necessary, particularly as regards criminal records and birth certificates. We also verified that DG HR had implemented our previous recommendations on the right of Commission staff to access their electronic personnel file after moving to another institution.

While we concluded that DG HR is essentially compliant with relevant data protection rules, we also outlined some recommendations for improvement. As with all other inspections, we will follow up on this case until all recommendations have been implemented.

Inspections are one of several tools used by the EDPS to monitor and ensure the application of the Regulation. Articles 41(2), 46(c) and 47(2) give the EDPS extensive powers to access any information, including personal data, necessary for his inquiries and the right to access any premises where the controller of the EU institution or body carries out its activity. Article 30 of the Regulation requires EU institutions and bodies to cooperate with the EDPS in performing his duties. The 2013 EDPS Inspection Guidelines contain the criteria the EDPS applies to launch an inspection and a 2013 Policy Paper on inspections further explains the EDPS' approach to inspections.

EDPS examines recruitment complaint

In 2015 we handled a complaint related to a request for access to personal data in a recruitment procedure at an EU body; the complaint concerned access to written feedback on the complainant's performance during the recruitment process.

In our Guidelines on the Rights of Individuals with regard to the Processing of Personal Data we recommend that *qualitative comments*, used to justify marks given in the recruitment process, be made available to those individuals concerned who request them. However, whilst

the EU body in question had provided the complainant with their marks for each evaluation section of the recruitment procedure, it failed to provide them with the reasons for these marks. The EU body claimed that this information had been made available orally and that providing these qualitative comments in writing would endanger the secrecy of the selection board proceedings.

As outlined in our Guidelines, the secrecy of the selection board's discussions is one of the reasons for which access to these comments can be denied. However, in this case, we judged this argument invalid. In making its comments available orally, the EU body had already decided that their availability was not compromising the secrecy of the selection board's discussions and therefore could not rely on this argument to justify their refusal to provide the comments in writing.

The EU body subsequently complied with our decision and provided the complainant with a paper copy of the comments requested.

One of the main duties of the EDPS, as established by Regulation (EC) No 45/2001, is to *hear and investigate complaints* as well as *to conduct inquiries either on his or her own initiative or on the basis of a complaint* (Article 46).

2.5.2 Whistleblowing

Whistleblowing made easy and data protection friendly

In 2015, the EDPS worked on a checklist to provide practical guidance to the EU institutions and bodies, both before and after the implementation of a whistleblowing procedure, to ensure that they comply with data protection obligations.

The checklist includes guidance on how staff can blow the whistle and how to ensure that the identity of staff members who blow the whistle is adequately protected. Confidence in this procedure is integral to ensuring that individuals do not hesitate to blow the whistle when necessary. The checklist also outlines what information can be processed and provides clarification on what types of data are classed as personal data.

The personal information in a whistleblowing report can relate to whistleblowers, the person under investigation, witnesses or other individuals that are mentioned. Each of these individuals must be informed as soon as practically possible that a whistleblowing procedure is underway and a general privacy statement should be published on each institution's website or intranet. Additionally, appropriate measures need to be implemented on the basis of a risk assessment to guarantee the security of whistleblowing files. The checklist will be available for use by the EU institutions and bodies in early 2016.

EDPS provides advice on whistleblowing procedures

It is a legal obligation, laid down in the Staff Regulations and included in the Conditions of Employment of Other Servants of the European Union, for all staff members to report fraud, corruption or other serious professional wrongdoing within the EU institutions and bodies. Whistleblowing procedures facilitate this and the Staff Regulations oblige the EU institutions and bodies to have such procedures in place.

In 2015, many EU institutions and bodies adopted internal rules on whistleblowing, following a call to do so by the European Ombudsman. These rules aim to safeguard the rights and interests of whistleblowers and provide adequate remedies if they are not treated correctly and fairly. In the various Opinions we issued on these procedures, we focused on preserving the confidentiality of all individuals involved in the whistleblowing process.

To encourage staff to blow the whistle, EU institutions and bodies must assure them that their identity will be protected. However, they must also ensure that the accused person is protected in the same manner as the whistleblower, in order to avoid stigmatisation and victimisation within their organisation. Confidentiality also depends on ensuring that appropriate security measures are implemented, including restricting access to both electronic and paper files and performing information security risk management. It is not only important to have security measures in place but to ensure that the security measures are the best ones for the case in question.

Though many of the Opinions are still in the follow-up phase, institutions are making good progress in implementing our recommendations.

Regulation (EC) No 45/2001 provides that all processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes are to be subject to prior checking by the EDPS (Article 27(1)).

2.5.3 Fraud

Investing in compliance: EDPS inspection at the EIB

In December 2015, the EDPS conducted an inspection at the European Investment Bank (EIB) in Luxembourg. The EIB is one of the EU's biggest institutions. It is mainly in charge of funding investment projects to support EU policy objectives.

The onsite inspection covered two main areas, fraud investigation and anti-harassment procedures, both of which involve the processing of sensitive data.

The inspection team conducted interviews with randomly-selected staff members in charge of specific fraud and harassment cases. For each case, the team verified the information collected, the data transfers carried out within and outside the EIB, the use of computer forensics by investigators and the conservation periods of the data collected during the investigations. We also addressed security matters, which involved a demonstration of the EIB's electronic files as well as a visit to their paper archives.

The exercise showed the EIB to be compliant with data protection rules. However, in order to be fully compliant, the EIB must implement our recommendations for improvement, which will be included in the inspection report. The EDPS will follow up on this case in 2016.

Due diligence at the EIF

In the course of 2015, the EDPS issued two Opinions on the processing of personal data at the European Investment Fund (EIF) in the context of *due diligence controls* on transactions and verifications on money-laundering and the financing of terrorism.

The EIF uses due diligence controls to assess the eligibility of companies (*financial counterparties*) to carry out private equity transactions with the EIF. These eligibility checks focus on the moral and professional requirements of management and other individuals involved with the financial counterparty.

In our Opinion of 10 July 2015 we referred to the need for the EIF to evaluate whether each and every search query they make on a financial counterparty is clearly and directly linked to the verification of their eligibility. We also advised them to adopt a more specific legal basis for these checks, authorising the processing of special categories of personal data, and to discontinue the processing of personal data relating to the age or health status of individuals working for the financial counterparty.

In an earlier Opinion, published on 13 May 2015, we found that similar measures should also be taken by the EIF when processing personal data for the purpose of avoiding business with companies involved in money-laundering or the financing of terrorism.

2.5.4 Cloud computing

Cloud computing is becoming the standard way of computing. Our personal data and, in particular, the data collected by private companies, will be increasingly stored online in large, networked data centres across the world. However, although data protection legislation provides the basic principles and obligations needed to protect personal data, cloud computing services are so complex and often involve such a large number of stakeholders that specific safeguards are necessary to ensure effective protection for users.

We worked with legislators, industry and the EU institutions and bodies throughout 2015 to provide advice on how to fully exploit the potential of cloud services while remaining in control of personal data. We advised EU institutions and bodies thinking about adopting cloud services to conduct a specific data protection impact assessment (DPIA) and, based on this assessment, to evaluate whether the potential risks could be adequately mitigated. This assessment should be reviewed periodically and especially if an important element of the assessment changes.

Once an institution decides to adopt cloud services it must translate the data protection and security requirements identified during the DPIA into requirements for the procurement process. These should then be integrated into the contract and Service Level Agreement (SLA). To help in this process, we have encouraged EU institutions and bodies to establish a common IT strategy on cloud computing in the form of a framework for SLAs.

@EU_EDPS

#responsibility must not vanish in the #clouds when processing personal information #eudatap @cspforum @Buttarelli_G

Work underway on Cloud Computing Guidelines

Cloud computing services are evolving fast. We have therefore been consolidating the advice we have provided to EU institutions and bodies in bilateral exchanges into guidelines which can be accessed and used by all. These will be finalised in 2016, after consultation with the institutions.

Our guidance will focus on common risks and relevant safeguards related to cloud computing, as well as on the need to conduct a risk assessment. It will also take stock of former guidance provided by the EDPS and the Article 29 Working Party (WP29), existing best practices and standards, including guidance from the European Network and Information Security Agency (ENISA), and the outcome of the ongoing work on the European Commission's Cloud Computing Strategy.

Cloud I comes under data protection scrutiny

The first inter-institutional Call for Tender for the provision of cloud-based services, Cloud I, was launched by the Commission's Directorate General for Informatics (DG DIGIT) at the end of 2014. It came to an end in 2015 and is now starting to deliver results.

We welcomed and contributed to the cautious approach taken to this project and will continue to support the Commission and the other institutions involved over the course of 2016. Our job will be to act as both an advisor and a prospective customer as we assess how the services offered by Cloud I comply with data protection requirements.

Constructing the Cloud Computing Code of Conduct

One of the elements of the Commission's Cloud Computing Strategy is a Data Protection Code of Conduct for Cloud Service Providers. This has been drafted by the Cloud Select Industry Group (CSIG) and was submitted to the Article 29 Working Party for assessment at the beginning of 2015.

@EU_EDPS

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

We were directly involved in reviewing the Code and contributed to the WP29 Opinion on the project, adopted in September 2015. The Opinion noted our appreciation for the effort made by industry in drafting the Code, as well as the crucial role of the Code and the progress made during the drafting process. However, the WP29 also highlighted many points which require improvement in order for the Code to be considered compliant with data protection rules.

2.5.5 Financial data

Over the course of 2015, we provided advice on the processing of personal data in the context of financial markets and services to both the European Commission's Directorate General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) and the European Central Bank (ECB).

The informal comments we provided to DG FISMA related to proposed legislation aimed at reforming securities markets, for example preventing market abuse and prospectus drafting, and the provision of financial services.

Our advice to the ECB focused on the adoption of a Regulation on the collection of credit information, including information on the provision of loans by national credit institutions.

2.5.6 DPO Network

Putting the Strategy into practice: the EDPS meets DPOs

The EDPS and the Data Protection Officers (DPOs) of the EU institutions and bodies met on two occasions in 2015: at the European Investment Fund (EIF) in Luxembourg in May and at the European Union Agency for Network and Information Security (ENISA) in Athens in November. Both meetings were chaired by Assistant Supervisor Wojciech Wiewiórowski. DPO meetings take place twice a year and have been a regular fixture in the EDPS calendar since 2004. They are an opportunity for DPOs to share experiences from their respective institutions and for the EDPS to present our policies and activities to DPOs.

We strongly believe in and value our cooperation with both DPOs and Data Protection Coordinators (DPCs). We support them and rely on them to act as a relay. The EDPS Strategy 2015-2019 calls on the EDPS to continue to support EU institutions and bodies in moving beyond a purely compliance-based approach to data protection to one that is also based on accountability. Our objective at the meetings in 2015, therefore, was to launch a new and innovative format for these meetings, making them more dynamic and interactive.

Both meetings were based on interactive workshops, where DPOs were given the opportunity to discuss challenging issues and receive hands-on advice. Topics of discussion in Luxembourg included the Guidelines on mobile devices (see section 2.2.2), accountability, security of processing, and the role of the DPO in the context of complaints. We discussed complaints again at the meeting in Athens, this time with a focus on case studies from both a legal and an IT perspective. We also undertook a collective intelligence exercise in view of the revision of our Guidelines on disciplinary matters, and dedicated one workshop to the relationship between information security and data protection. The new format proved very successful and, in light of the positive feedback we received, we plan to organise our meetings in 2016 in a similar fashion.

In addition to these meetings, we also set up an informal working group, including a number of DPOs, to share views on the revision of Regulation 45/2001 in light of the reform of EU data protection rules. Our discussions focused mainly on accountability and the role of the DPO. We will continue this exercise in 2016, with discussions on topics of particular relevance for DPOs.

DPO training in information security

The topic of information security was discussed at both DPO meetings in 2015. DPOs were encouraged to reflect upon the relationship between information security and data protection and how, without adequate information security, there cannot be any data protection.

We also discussed the risk management process, which forms the basis of information security, and how and why DPOs should be involved in this process. The workshops were considered a success and were well-attended. As the topic is very important and complex, we plan to cover it again in future DPO meetings.

3. Court Cases

In 2015, the EDPS was involved in a range of high-profile cases which resulted in important rulings. These rulings have both helped us to more clearly define data protection law and to ensure that the fundamental right to privacy and data protection is fully respected.

Transparency and data protection: a balancing act

In July 2015, the Court of Justice of the EU (CJEU) ruled on two cases related to transparency and data protection. The judgments provided some clarity on how to reconcile the need for transparency and openness in the EU bodies with the fundamental right to data protection.

EU citizens have the right to request access to documents from EU public bodies in the interest of transparency and openness. However, EU institutions and bodies have an obligation to protect the personal data of individuals which might appear in these documents. It is, therefore, important to clarify under which circumstances the protection of personal data should prevail.

In Case T-115/13, Dennekamp v. European Parliament, the General Court found that the right to information and the right to freedom of expression were not sufficient reasons to warrant the transfer of personal data of Members of the European Parliament (MEPs) to a journalist. The possibility of uncovering conflicts of interest, however, was considered sufficient. Supported by the EDPS, Mr. Dennekamp had argued that the public interest in transparency warranted access to information about MEPs affiliated to a now defunct pension scheme.

In Case V-615/13, ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA), in which the EDPS also intervened, the Court of Justice ruled that the identity of external experts who had commented on a draft guidance document produced by EFSA should be made available, on the basis that increased transparency demonstrates the impartiality of the experts in question. It was considered that this kind of transparency in EU decision making was necessary to ensure that EU institutions remain accountable to the citizens they serve.

Under EU data protection rules, access to personal data can only be given when it can be shown that the transfer of personal data meets the criteria of necessity and proportionality and provided that the individual's legitimate interests are not prejudiced by the disclosure. The cases gave an insight into the arguments which meet these criteria and the arguments that do not, allowing us to further define and understand the relationship between data protection and transparency.

@EU_EDPS

#EUdataP and #transparency go hand in hand serving the interests of the #individual #antifraud @Buttarelli_G

Parliament, petitions and personal data

On 24 March 2015, the EDPS pleaded before the General Court of the European Union in Case T-343/13 concerning the handling of petitions by the European Parliament. The plaintiff accused the Parliament of having unlawfully published his personal data on the European Parliament website when handling his petition.

The EDPS intervened in support of the plaintiff. We reaffirmed that data protection applies in the context of all political activities conducted by the European

Parliament, including the publication of petitions. In particular, we observed that the Parliament's own Rules of Procedure do not require that the petitions submitted to it be published in full.

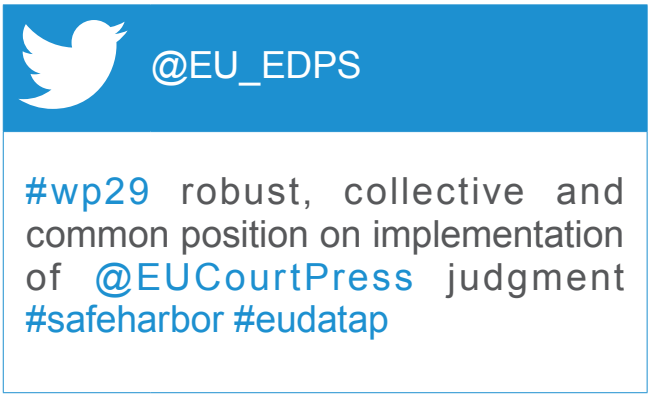
We argued that, with sensitive health data at stake, the Parliament should have provided the petitioner with specific details about how his information would be published and informed him that he could submit a redacted text for publication. Furthermore, the Parliament should have evaluated the risks associated with publishing personal data related to someone other than the petitioner. In this case, personal data relating to the health of the petitioner's son should not have been published. As the Parliament website is indexed by external search engines, all personal information published there is vulnerable to wide, possibly irreversible, and decontextualised dissemination in the public domain. We argued that the Parliament's approach should have been to find a balance between transparency and data protection.

The Court's judgment, published on 3 December 2015, followed the same legal reasoning used by the EDPS. However, the Court considered that the information provided by the Parliament to the petitioner when requesting consent for the publication of his personal data was appropriate and that the petitioner's consent was therefore given. The case was consequently dismissed. The claim relating to the personal data of the petitioner's son was also dismissed, as the petitioner could not show that he acted as a representative for or on behalf of his son in the judicial proceeding.

EU Court declares safe harbour agreement invalid

On 24 March 2015, the EDPS intervened before the Court of Justice of the European Union at the hearing of Case T-343/13 Maximillian Schrems v Data Protection Commissioner. The EDPS is not admitted to intervene in preliminary ruling procedures and was therefore not a party to the case. The Court is, however, entitled to ask the EDPS to submit observations on the case in its role as advisor to the European institutions on data protection.

The case concerned the Safe Harbour arrangement, negotiated by the European Commission more than 15 years ago to ensure that personal data transferred from the EU to the US received the same level of protection as it would in the EU. Though it was not the only way to transfer data between the two, it was widely used. Many large American technology companies transferred data on the basis of this arrangement, including Facebook.



The Irish Data Protection Commissioner received a complaint related to transfers of personal data by Facebook Ireland Ltd. to the servers of its US parent company, Facebook Inc. The complainant argued that personal data transferred to the US in the context of the Safe Harbour framework was not adequately protected. He drew on the recent revelations of mass surveillance as evidence to support his argument. As the Irish data protection authority (DPA) considered itself unable to act on the Safe Harbour decision, the complainant took his case to the High Court of Ireland, which referred a number of questions to the CJEU.

In our observations to the CJEU, we made the following points:

- There have long been doubts about Safe Harbour; despite the Article 29 Working Party's (WP29) consistent criticisms on a number of weaknesses, these have not been resolved;
- The reach and scale of surveillance may be so broad that Safe Harbour failed to respect the essence of the fundamental rights to privacy and data protection enshrined in the Charter of Fundamental Rights;
- Independent data protection authorities have the power to determine what actions are necessary to ensure a fair balance between privacy and the protection of personal data and, in the present case, disruption to the internal market.

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

On 6 October 2015, the CJEU declared the European Commission's Safe Harbour decision invalid. The Court's decision followed the opinion of Advocate

General Bot, given on 23 September 2015. It found that, due to the threat of US mass surveillance, personal data transferred to the US under the arrangement was not adequately protected. The transfer of personal data through this process was therefore ruled illegal.

In its judgment, the Court clarified that, when negotiating an adequacy decision such as Safe Harbour, the Commission is obliged to assess both the content of the data protection rules in the country in question and the measures designed to enforce compliance with these rules. This assessment should be repeated on a regular basis to ensure that the rules in place continue to provide for a level of data protection which is essentially equivalent to the one that exists in the EU. The Court also ruled that national DPAs have the authority to examine complaints relating to the Commission's adequacy decisions. National DPAs can therefore investigate the level of protection provided by an adequacy decision and challenge its validity on behalf of any individual who raises concerns.

4. Transparency and Access to Documents

As an EU institution and according to its Rules of Procedure, the EDPS is subject to the Public Access to Documents Regulation of 2001. Though the number of public access requests for documents held by the EDPS has increased progressively over the years, this year the number fell significantly from 18 requests in 2014 to five requests in 2015.

We will continue to respond to requests for public access to documents throughout 2016 and to increase the transparency of our work. This will include projects such as continuing to update the EDPS website, making it more accessible and increasing the amount of information available on it.

5. The Secretariat

5.1 INFORMATION AND COMMUNICATION

The new EDPS mandate has initiated a new approach to EDPS communication as we strive to achieve the vision outlined in our Strategy 2015-2019 of an EU which leads by example in the global dialogue on data protection and privacy.

Central to this process has been the development of a new image for the institution. This began in May 2015 with the launch of a new logo and was followed in November 2015 by the re-launch of the EDPS website. This process is set to continue into 2016 with a fundamental update to the website.

We also introduced new communications tools, including the EDPS app on the General Data Protection Reform, through which we were able to make the legislative process more transparent and ensure that the legislators could be held more accountable for their decisions.

5.1.1 Online media

Website

2015 saw the beginning of a project designed to make the EDPS website more user-friendly and fit-for-purpose. The new-look website was launched in November 2015 and incorporates a variety of new features, including an agenda, a responsive design for use on smartphones and tablets and a new layout for the homepage, all aimed at increasing transparency and accessibility. This process will continue in 2016.

Though the number of new visitors to the website decreased in 2015, this is unsurprising as much of the first part of 2015 was focused on establishing the aims of the new mandate. This meant that there were fewer new activities to report on the website. However, the total number of visitors to the website increased, indicating that established users continue to turn to the EDPS as a source of information and expertise on data protection.

Social media

Social media is an increasingly important communications tool for the EDPS. Our growing success on these platforms demonstrates our increasing global influence as an authority on data protection.

Twitter (@EU_EDPS) remains our most influential social media tool. We witnessed a dramatic increase in followers in 2015 and tweeted more than twice as much as in 2014.

We also strengthened our online presence and visibility through LinkedIn. Our increasingly interactive presence on the site, which we use to promote EDPS activities, events and news, led to a significant increase in followers as well as a high average engagement rate of 2.87% of followers with each of our posts.

YouTube has also become a valuable tool, allowing us to promote EDPS videos to a wider audience. Our increasing effectiveness on this platform is demonstrated by the number of views of EDPS videos, which increased by over 356% in comparison to 2014.

EDPS mobile app on the General Data Protection Regulation

@EU_EDPS

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

In July 2015 we released a mobile app which allowed users of different platforms to compare EDPS recommendations on the General Data Protection Regulation (GDPR) with the texts produced by the Commission, the Parliament and the Council. By the end of 2015, the app had been downloaded 2948 times. It proved an innovative way for the EDPS to encourage the legislators to implement pragmatic solutions and contributed to the transparency and accountability of the legislative process.

5.1.2 New visual identity

EDPS Logo

In May 2015, we launched a new EDPS logo. This was part of a process to develop a new visual identity for the institution, to reflect a new era in the history of the EDPS as a global leader in data protection and privacy.

The logo itself comprises three components. The flag symbolises the institution's strong relationships and integration with other EU institutions and bodies and data protection authorities while the wave of binary code reflects the EDPS' role as the European guardian of data protection, as well as its strength as a dynamic institution that continues to grow in importance and influence.

@EU_EDPS

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

Media relations

Over the course of 2015, the EDPS issued 13 press releases. All of these were published on the EDPS and EU Newsroom websites and were distributed to our network of journalists and other interested parties. In addition to this, we answered 31 written media enquiries and the EDPS and Assistant EDPS gave 39 direct interviews to European and international journalists.

The slight decrease in these figures in comparison to 2014 combined with the dramatic increase in our use of social media reflects our attempts to better focus our media relations strategy to achieve maximum impact for our most influential activities. The success of this strategy has led to significant media coverage over the year, particularly in relation to Safe Harbour, Passenger Name Records (PNR) and the GDPR. The EDPS appeared in over 400 articles, radio broadcasts, videos or other media in 2015, ensuring that our Opinions and advice reached a wide audience.

5.1.3 Events and publications

EDPS Strategy 2015-2019

@EU_EDPS

#EDPS Strategy 2015-2019 official launch today @EU_Commission @EP_Justice @EUCouncil with @TimmermansEU @ClaudeMoraes

On 2 March 2015, EDPS Giovanni Buttarelli presented the EDPS Strategy 2015-2019 at an event for senior representatives of the EU, together with Assistant Supervisor Wojciech Wiewiórowski and EDPS Director Christopher Docksey. The Strategy outlines the main

objectives for the current mandate and the actions the EDPS will take to turn this vision into a reality. In combination with our new visual identity, it has proved a valuable tool in establishing the position and intentions of the EDPS in relation to current and future data protection and privacy challenges.

EU Open Day 2015

On Saturday 9 May we participated in the annual Open Day of the EU institutions and bodies in Brussels. This is an opportunity to increase general public awareness of data protection and the role of the EDPS.

Our stand, located in the European Parliament, proved more popular than ever. Visitors were able to interact with facial detection and online tracking software and EDPS staff were on hand to answer questions. There were also promotional items available for the 663 visitors who completed our data protection quiz.

Newsletter

We published three editions of the EDPS Newsletter in 2015 on our website, which were also sent to out to our Newsletter mailing list. The number of subscribers to our Newsletter continues to grow, demonstrating the continued importance of the EDPS Newsletter for communicating our most recent activities.

5.1.4 External relations

Study visits

In 2015 we organised seven study visits for groups from European universities and youth organisations. These visits allow us to interact directly with young people, raising awareness of data protection and the work of the EDPS.

Information requests

The number of public information requests received by the EDPS decreased in 2015. This was due to the increasingly effective communication of our messages and our competencies, the latter leading to a decrease in the number of requests wrongly addressed to the EDPS.

The majority of queries we received concerned requests for information on privacy matters or assistance in dealing with problems related to the protection of personal data, as well as to matters over which the EDPS has no competence. We replied to all requests with information relevant to the individual enquiry.

5.2 ADMINISTRATION, BUDGET AND STAFF

2015 has been a challenging year for the EDPS. The development of a new Strategy, the change in leadership and a heavy workload with a shrinking budget put pressure on EDPS staff. Nevertheless, we successfully overcame these challenges and are now ready to pursue the ambitious goals of the new mandate with a team of young, dynamic and highly motivated EU officials.

In 2015 we received a clean bill of health from the Court of Auditors for the fourth consecutive year and we further improved the implementation rate of our budget. We have also invested resources in strengthening our limited procurement capabilities.

A range of new Human Resources (HR) policies were also adopted in 2015, in areas such as Learning and Development (L&D), career guidance and equal opportunities. We have also substantially improved the level of EDPS accountability through the adoption of a Code of Conduct for the Supervisors and a decision on internal rules on whistleblowing.

Lastly, with the cooperation of EPSO and data protection colleagues from other EU institutions and bodies, we invested significant time and resources in organising a specialist competition for data protection experts. This resulted in a reserve list of 21 candidates which will cover the recruitment needs of the EDPS and the future European Data Protection Board (EDPB) in the short and medium term.

5.2.1 Budget and finance

Budget

In 2015, the EDPS was allocated a budget of EUR 8 760 417. This represents an increase of 1.09% compared to the 2014 budget. Quarterly reviews of our budget implementation have allowed us to achieve better implementation rates: from 85% in 2011 to around 94% in 2015.

For the third consecutive year, we followed the austerity guidelines provided by the Commission and maintained our policy of budget consolidation. Nevertheless, some additional resources were requested for new activities foreseen in the EDPS Multiannual Financial Framework 2014-2020 (MFF 2014-2020). One of the most significant activities was the creation of a small task-force by mid-2015, with the responsibility of assessing the necessary legal, operational and budgetary means for the future set up of the European Data Protection Board (EDPB).

The selection of a new team of Supervisors in late 2014 meant that some of the credits requested to cover temporary allowances became unnecessary. An amending budget to return the unused credits to the general EU budget was therefore submitted and approved by the budgetary authority in October 2015.

Finance

There were no concerns or recommendations addressed to us in the Statement of Assurance from the Court of Auditors for the financial year 2014 (DAS 2014). The EDPS obtained a clean bill of health for the fourth consecutive year.

The Commission continued to assist us in finance matters. In the area of accountancy services, for example, the Accounting Officer of the Commission remains the Accounting Officer of the EDPS.

Procurement

In addition to updating the section on Budget and Finance on the EDPS intranet, we also added a specific section on procurement. This includes a list of

inter-institutional framework contracts in which the EDPS participates as well as a detailed check-list for staff on how to make requests for supplies or service contracts.

The EDPS benefits from being party to many inter-institutional framework contracts. This has allowed us to conclude specific contracts related to major IT projects in 2015, such as website development, an Information Security policy and the analysis of IT needs for the future EDPB.

We also met twice with the finance team of the European Ombudsman in 2015 to identify common needs. Closer collaboration is foreseen for 2016.

5.2.2 Human resources

New policies

Learning and development (L&D): Further to the new strategy on L&D adopted in 2014, a new administrative Decision on L&D was adopted in July 2015, implementing the principles of the new EDPS Strategy 2015-2019 and strengthening support for learning. Each staff member now has a personal L&D Plan, which should allow us to adopt a longer term perspective on the learning and development needs of EDPS staff.

Tailor-made trainings, conducted in-house and customised to the needs of specific EDPS staff members have also been organised, on topics such as public speaking and media training, KPIs and impact assessment. They have been highly appreciated by our staff and represent a good return on investment for the institution.

We also launched the first short secondment and exchange programme in February 2015, designed to strengthen links with some of our stakeholders and provide valuable professional experience to the staff members participating. Two projects were selected for the 2015-2016 session.

Career guidance: A new policy on career guidance was adopted in 2015. HR Management aims to have the right person in the right job at the right time and sound career guidance is essential in this regard.

In 2016 we will appoint a Local Career Guidance Officer (ReLOp) to provide services such as guidance in career planning, assistance in case of reintegration after a long absence or to support staff and management in scenarios where mobility is identified as a possible solution.

Decision on underperformance: In line with the new staff regulations, we adopted a decision on underperformance on 10 November 2015.

The decision includes a *prevention phase*, which should be intiated if a line manager identifies a staff member as being at risk of performing in an unsatisfactory manner. This involves setting up an Action Plan outlining steps to be taken, success criteria and a calendar.

Under normal circumstances, the Action Plan should make launching the underperformance procedure unnecessary. However, if the prevention phase is not successful, underperformance must be mentioned in the official's evaluation report. After three consecutive unsatisfactory reports, an official can be downgraded. After five consecutive unsatisfactory reports they can be dismissed.

Equal opportunities: A draft EDPS equal opportunities strategy was submitted to the Management Board in December 2015. It sets out three objectives: maintaining a balanced workforce; preventing discrimination and harassment; and accommodating the needs of all employees. The goal is to enable each employee to fulfil their potential.

The barriers to equal opportunities are examined at three levels: selection; working conditions; and culture. Policies to overcome these barriers are proposed.

Our next steps will be to consult staff about the contents of the proposed strategy, assess the key issues facing equal opportunities through a staff satisfaction survey and mainstream equal opportunities into HR activities to monitor progress.

Accountability

Whistleblowing: In December 2015 we adopted a decision on internal rules concerning whistleblowing. Under the Staff Regulations of the European Institutions, staff are obligated to report any serious irregularities, misconduct or negligence witnessed when performing their duties. The rules outlined in the decision aim to inform staff members on whistleblowing and give clear instructions on how to blow the whistle.

Code of Conduct for the Supervisors: A Code of Conduct for the European Data Protection Supervisor and the Assistant Supervisor was adopted at the last Management Board meeting of 2015. It serves as a reference point for EDPS stakeholders and for the general public, allowing them to hold the Supervisors accountable for integrating ethical insights into their daily work, in the spirit of the new EU institutional framework and the Lisbon treaty.

The document builds on best practices, particularly from national data protection authorities and other European institutions. It also reflects the principles enshrined in the Rules of Procedure of the EDPS and the EDPS staff Code of Conduct.

Compliance with data protection: The new Staff Regulations of officials and other agents of the European Union, adopted in 2014, as well as the subsequent adoption of implementing decisions, made it necessary to conduct an in-depth review of all data protection notifications issued to our Data Protection Officer. This review of 19 notifications concerning the processing of personal data in the field of human resources and finance adapts all references to the new legal framework and builds on our commitment to ensure that all obligations specified in the notifications are effectively complied with and put into practice.

After completing this in-depth review, it was possible to consolidate all data retention periods applicable to processing operations by the Human Resources, Budget and Administration (HRBA) unit at the EDPS into a single table. This new table will facilitate a regular review of retention times in our human resources and finance files leading to better compliance in practice.

Knowledge management and internal communication: We invested considerable time and resources in the area of knowledge management and internal communication in 2015. Our section on the EDPS Intranet was fully reviewed and updated and a new manual on HRBA filing and knowledge management was developed.

5.2.3 European Data Protection Board (EDPB)

At the end of 2015, the Council and the European Parliament reached a political agreement on the text of the General Data Protection Regulation (GDPR). This new legal framework, which will enter into force in 2018, involves setting up a new EU body: the EDPB. The EDPB will be fully independent but, administratively, the EDPS will provide its Secretariat.

In cooperation with colleagues in the Article 29 Working Party (WP29), we have been preparing administratively for the future EDPB since 2013. This may include adapting existing or signing new Service Level Agreements with larger EU institutions and bodies so that the EDPB can fully benefit from essential services such as translation and interpretation. A small internal EDPS Task Force was created in late 2015, which may gradually be reinforced in 2016 and 2017. We also contribute to a separate task force with colleagues of the WP29. The relevant EDPS staff will make preliminary analyses to assist with the challenging task of setting up the Board so that it can be fully operational from day one.

5.2.4 A competition for data protection specialists

In order to cover the recruitment needs of the EDPS and the future EDPB, we asked EPSO to organise a competition for data protection specialists. The official notice was published in October 2014. The selection process required candidates to pass official tests. The selection board, which included six EDPS staff members and a number of data protection colleagues from other EU institutions and bodies, then worked hard to identify the successful candidates. The outcome was a reserve list of outstanding data protection experts that was published in the Official Journal in July 2015. Two laureates were recruited in 2015 and more may be recruited in 2016.

6. The Data Protection Officer at the EDPS

6.1 THE DPO AT THE EDPS

In the EDPS, as in other EU institutions and bodies, the Data Protection Officer (DPO) provides guidance and helps to ensure the institution's compliance with personal data protection rules. However, the EDPS DPO faces some additional challenges. These include meeting the expectations of colleagues who are data protection experts and delivering solutions that can serve as benchmarks for other institutions.

6.2 LEADING BY EXAMPLE

In line with our supervision policy and the EDPS Strategy 2015-2019, in 2015 the EDPS DPO initiated a project to develop an accountability framework, involving both data protection and human resources colleagues. This framework will be used in the institution to ensure more effective protection of personal data and to anticipate legal requirements which it will be necessary to adhere to in the future. It will also be presented to the second meeting of DPOs in 2016 as a practical example of how to implement accountability.

6.3 ADVISING THE INSTITUTION AND IMPROVING THE LEVEL OF PROTECTION

In 2015 the DPO provided advice on a number of planned processing operations and new internal policies at the EDPS. These included a reporting tool for human resources, the EDPS whistleblowing policy, our personal data breach procedure and our record management policy.

In order to increase the level of data protection in practice at the EDPS, the DPO also both organised the provision of new scanning devices, which allow staff to send personal documents, including medical documents, directly to staff mailboxes, and worked on ensuring the protection of personal data for users of the EDPS website.

6.4 THE REGISTER OF PROCESSING OPERATIONS

Under Article 26 of the Regulation, the DPO must keep a register of notifications for all EDPS operations which involve the processing of personal data.

In 2015, the DPO ensured that 19 notifications relating to the processing of personal data in finance and human resources work were updated, taking into account the staff reform and consequent changes in relevant legal provisions.

6.5 PROVIDING INFORMATION AND RAISING AWARENESS

It is of the utmost importance to ensure that all staff involved in processing personal data at the EDPS are aware of the role of the DPO and the activities carried out by the DPO. The DPO uses several tools to raise awareness.

As part of their welcome, newcomers to the EDPS attend a data protection induction course organised by the DPO. The meetings are tailored according to staff expertise and the role they will perform at the EDPS.

Additionally, the DPO section on the EDPS intranet contains information that is useful for staff, including a detailed list of privacy statements with all the relevant details of EDPS processing operations. This allows staff to stay informed and ensures that they have the necessary tools to exercise their data protection rights, should they need to do so. Internal EDPS coordination and information meetings are also opportunities to reach out to all staff.

There is also a dedicated DPO section on the EDPS website. This offers information about the role and activities of the DPO and is updated regularly to ensure that the register and all notifications are publically available.

The twice-yearly meetings of the DPOs of the EU institutions and bodies represent a unique opportunity for the EDPS DPO to discuss common issues and share experiences and best practices with DPO colleagues. In 2015, the meetings took place in Luxembourg in May and in Athens in November. They included helpful discussions and workshops on topics such as accountability, IT security, data protection impact assessments, privacy by design, disciplinary matters and personal data, and the right to access and publication of personal data (see section 2.5.6).

7. Main Objectives for 2016

The following objectives have been selected for 2016 within the overall Strategy for 2015-2019. The results will be reported in 2017.

Data protection goes digital

The General Data Protection Regulation (GDPR) will create an obligation for controllers to implement data protection principles and safeguards in the development and operation of data processing systems. With this legal obligation, the importance of *data protection by design and by default* will increase. Providing guidance on the technical implementation of data protection will become an increasingly important task for all supervisory authorities, including the EDPS.

Increasing transparency, user control and accountability in big data processing

There is a need for the EU to develop a model for information-handling policies for online services provided by EU institutions and bodies. Using clear and simple language, such policies should explain how business processes could affect individuals' rights to privacy and data protection. Citizens should also be told about whether they risk being re-identified from anonymous, pseudonymous or aggregated data. To this end, the EDPS will work with a special focus on data vaults and personal data stores.

Mainstreaming data protection into international policies

Part of the mission of the EDPS is to provide advice to the EU institutions and bodies on aspects of globalisation where privacy and data protection are becoming increasingly important. In cooperation with data protection authorities (DPAs), we will provide advice on how established EU data protection principles can be applied coherently and consistently whenever EU representatives are negotiating trade agreements, or international agreements linked to law enforcement, taking care to highlight the positive effects of EU data protection principles in facilitating global trade and law enforcement cooperation. We therefore plan to closely follow agreements such as the Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TISA). We also plan to issue our own Opinion on international transfers in the wake of the invalidation of the Safe Harbour rules by the Court of Justice, to be coordinated with the Opinion of the Article 29 Working Party (WP29), of which we are a member, and to provide an assessment of the EU-US Umbrella Agreement in the area of law enforcement cooperation.

Speaking with a single EU voice in the international arena

The EDPS is determined to contribute to the emergence of a global alliance with data protection and privacy authorities worldwide. In collaboration with the WP29, our aim is to identify technical and regulatory responses to key challenges to data protection, such as big data, the internet of things and mass surveillance.

Revision of Regulation 45/2001

Now that the GDPR has been finalised, Regulation 45/2001 must be adapted to ensure that the data protection laws applicable to the EU institutions and bodies remain in line with those applicable to the Member States. The EDPS plans to issue informal advice and an Opinion on the revision of the Regulation. We will also help EU institutions and bodies to adapt to the new rules, through continuing to train Data Protection Officers (DPOs) and controllers on the new requirements.

Accountability project

The EDPS has embraced and supported the concept of accountability, which is central to the data protection reform. We will continue asking EU administrations to be proactive in ensuring compliance and to properly document the measures taken so as to demonstrate compliance if necessary. In our efforts to lead by example, we will cooperate internally with the EDPS DPO to ensure that the accountability principle is effectively implemented within our own institution. DPOs and DPCs (Data Protection Coordinators/ Contacts) are integral to achieving this and we will therefore develop further training and guidance for them, encourage close contacts with and within the DPO Network and brief them on how the EDPS has implemented the accountability principle.

Preparing for Europol

A new data protection framework for Europol will enter into force in early 2017. This will require the EDPS to develop supervision activities, in cooperation, to a certain extent, with national authorities. The EDPS is currently preparing for this new role at organisational and human resources level and will continue to do so throughout 2016. Specific training and cooperation activities will be set up to help determine how best to conduct the supervision and coordination activities required by the regulation.

We will also continue to participate actively in international and regional data protection networks, in the Council of Europe and the OECD as well as the annual Computers, Privacy & Data Protection (CPDP) conference. Workshops with international organisations will be held on an ad-hoc basis, whenever international organisations are interested in sharing knowledge with the EDPS and in developing good practice together.

Preparing for the EDPB

Since the EDPS will provide the Secretariat for the European Data Protection Board (EDPB), we need to ensure that this body will be ready on day one. This preparatory work will be done in close cooperation with national authorities, through the WP29 and the WP29-EDPB taskforce and according to the plan adopted by the WP29. In this way we will ensure that proper transitional arrangements are in place for a seamless handover from the WP29. This work will include ensuring that we have an appropriate IT infrastructure, establishing working methods and rules of procedure and ensuring adequate human and financial resources. This will be achieved through close cooperation between the Policy unit, the Human Resources, Budget and Administration (HRBA) unit and the IT Policy sector.

Coordinated supervision

There is a need to ensure more effective and coordinated supervision of large-scale IT systems in the field of law enforcement, both at EU and national levels. We should also encourage legislators to harmonise the existing platforms, which are rather diverse. As Secretariat of the Coordinated Supervision Groups for several large-scale IT systems, we will continue to organise and support group and subgroup meetings on these systems throughout 2016. We also plan to launch a new website for the Groups which will help in achieving our aims.

Advising and supervising large scale IT systems

In response to current challenges in areas such as public security and border control, legislators have advocated the creation of new IT systems or the enhancement and functional extension of existing ones. We will provide policy makers and legislators with advice on the technological elements of these systems and develop our monitoring and supervision activities to ensure that the operations performed by these systems remain in line with data protection rules.

Promoting a mature conversation on security and privacy

For terms such as *national security*, *public security* and *serious crime* to be meaningful, and to therefore ensure that data protection principles are respected, the EU needs an informed discussion on their definition and scope. We intend to foster such a discussion in 2016, including a special focus on Smart Borders.

IT security

The importance of IT security continues to increase. We will further develop our expertise in this area in 2016 and, through our inspection and auditing activities, ensure that the relevant rules are applied. We will continue to act as a partner to all members of the IT security community with a particular focus on the EU institutions and bodies.

Guidance on technology and data protection

In addition to the 2015 Guidelines on the use of mobile devices, further Guidelines on web services, mobile apps and cloud computing will be concluded in 2016. These will be complemented by guidance on specific areas such as accountability in IT management and risk management.

Internet Privacy Engineering Network (IPEN)

This network of technology and privacy experts from DPAs, industry, academia and civil society will be required to play an important role in translating new data protection obligations into engineering requirements, supporting data protection by design. We will support the network as it intensifies its efforts to produce tangible results.

Identifying cross-disciplinary policy solutions

In 2016 we intend to encourage a Europe-wide dialogue on big data, the internet of things and on fundamental rights in the public and private sector. To achieve this, we will reach out to EU institutions, regulators, academics, industry, the IT community, consumer protection organisations and others as we organise a big data workshop and prepare and publish a paper on data protection and the Digital Single Market.

Technology monitoring

Our technology monitoring activities will become more visible and be made accessible to other stakeholders, making them more influential. A report will be made available to the public in addition to DPAs and technology-oriented expert groups at EU-level.

Facilitating responsible and informed policymaking

The EDPS plans to develop a comprehensive toolkit which will enable EU institutions and bodies to take informed decisions on data protection. We will also prepare written guidance, workshops and training events with the support of an external network. Additionally, each year, the EDPS will identify the EU policy issues with the most impact on privacy and data protection. We will then provide appropriate legal analysis and guidance on these issues.

The EDPS will continue to work towards establishing efficient working methods with the Parliament, Council and Commission and will actively seek feedback on the value of our advice. We are also committed to developing our dialogue with the Court of Justice of the EU on fundamental rights and to assisting the Court in all relevant cases, whether as a party or an expert.

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.

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

Other relevant EU acts on data protection are Directive 95/46/EC, which lays down a general framework for data protection law in the Member States, Directive 2002/58/EC on privacy and electronic communications (as amended by Directive 2009/136) and Council framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. These three instruments can be considered as the outcome of a legal development which started in the early 1970s in the Council of Europe.

Background

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms provides for a right to respect for private and family life, subject to restrictions allowed only under certain conditions. However, in 1981 it was considered necessary to adopt a separate convention on data protection, in order to develop a positive and structural approach to the protection of fundamental rights and freedoms, which may be affected by the processing of personal data in a modern society. The convention, also known as Convention 108, has been ratified by more than 40 Member States of the Council of Europe, including all EU Member States.

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

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

Regulation (EC) No 45/2001

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

The definitions and the substance of the Regulation closely follow the approach of Directive 95/46/EC. It could be said that Regulation (EC) No 45/2001 is the implementation of that directive at European level. This means that the Regulation deals with general principles

like fair and lawful processing, proportionality and compatible use, special categories of sensitive data, information to be given to the data subject, rights of the data subject, obligations of controllers — addressing special circumstances at EU level where appropriate — and with supervision, enforcement and remedies. A separate chapter deals with the protection of personal data and privacy in the context of internal telecommunication networks. This chapter is the implementation at European level of the former Directive 97/66/EC on privacy and communications.

An interesting feature of the Regulation is the obligation for EU institutions and bodies to appoint at least one person as Data Protection Officer (DPO). These officers have the task of ensuring the internal application of the provisions of the Regulation, including the proper notification of processing operations, in an independent manner. All institutions and most bodies now have these officers, and in some cases already for many years. These officers are often in a better position to advise or to intervene at an early stage and to help to develop good practice. Since the DPO has the formal duty to cooperate with the EDPS, this is a very important and highly appreciated network to work with and to develop further (see section 2.5.6).

Tasks and powers of EDPS

The tasks and powers of the EDPS are clearly described in Articles 41, 46 and 47 of the Regulation (see Annex B), both in general and in specific terms. Article 41 lays down the general mission of the EDPS — to ensure that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data are respected by EU institutions and bodies. Moreover, it sets out some broad lines for specific elements of this mission. These general responsibilities are developed and specified in Articles 46 and 47 with a detailed list of duties and powers.

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

Some tasks are of a special nature. The task of advising the Commission and other institutions about new legislation — emphasised in Article 28(2) by a formal obligation for the Commission to consult the EDPS when it adopts a legislative proposal relating to the protection of personal data — also relates to draft directives and other measures that are designed to apply at national level or to be implemented in national law. This is a strategic task that allows the EDPS to have a look at privacy implications at an early stage and to discuss any possible alternatives, also in areas that used to be part of the former *third pillar* (police and judicial cooperation in criminal matters). Monitoring relevant developments which may have an impact on the protection of personal data and intervening in cases before the Court of Justice are also important tasks.

The duty to cooperate with national supervisory authorities and supervisory bodies in the former *third pillar* has a similar, more strategic impact. As a member of the Article 29 Data Protection Working Party, established to advise the European Commission and to develop harmonised policies, the EDPS has the opportunity to contribute at that level. Cooperation with supervisory bodies in the former *third pillar* allows him to observe developments in that context and to contribute to a more coherent and consistent framework for the protection of personal data, regardless of the *pillar* or the specific context involved.

Annex B - Extract from Regulation (EC) No 45/2001

Article 41 — European Data Protection Supervisor

1. An independent supervisory authority is hereby established referred to as the European Data Protection Supervisor.

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

The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47.

Article 46 — Duties

The European Data Protection Supervisor shall:

(a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;

(b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;

(c) monitor and ensure the application of the provisions of this regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;

(d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;

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

(f) cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body;

ii) also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;

(g) participate in the activities of the working party on the protection of individuals with regard to the processing of personal data set up by Article 29 of Directive 95/46/EC;

(h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);

(i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the data protection officers under Article 26;

(j) carry out a prior check of processing notified to him or her;

(k) establish his or her rules of procedure.

Article 47 — Powers

1. The European Data Protection Supervisor may:

   (a) give advice to data subjects in the exercise of their rights;

   (b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;

   (c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;

   (d) warn or admonish the controller;

   (e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;

   (f) impose a temporary or definitive ban on processing;

   (g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;

   (h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;

   (i) intervene in actions brought before the Court of Justice of the European Communities.

2. The European Data Protection Supervisor shall have the power:

   (a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;

   (b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this regulation is being carried out there.

Annex C - Supervision and Enforcement activities

Prior Checks

In 2015, we received 65 notifications for prior checking, a fall of 18.75% compared to 2014. Progress was made in clearing the back-log of *ex-post* notifications received in 2013.

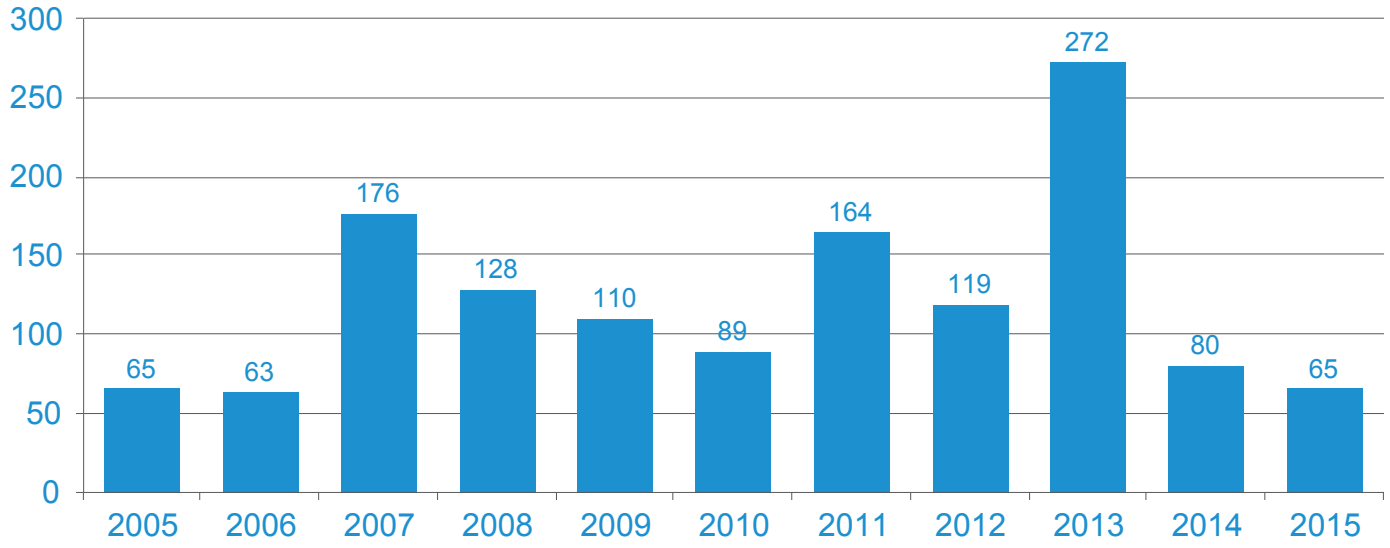


Fig. 1. Evolution of Notifications received by EDPS.

In 2015, we issued 67 prior check opinions (a decrease of approximately 53% from 2014). Of these, 7 were joint Opinions covering 21 notifications. We also issued 3 Opinions (an 88% decrease from 2014) on *non prior checks*.

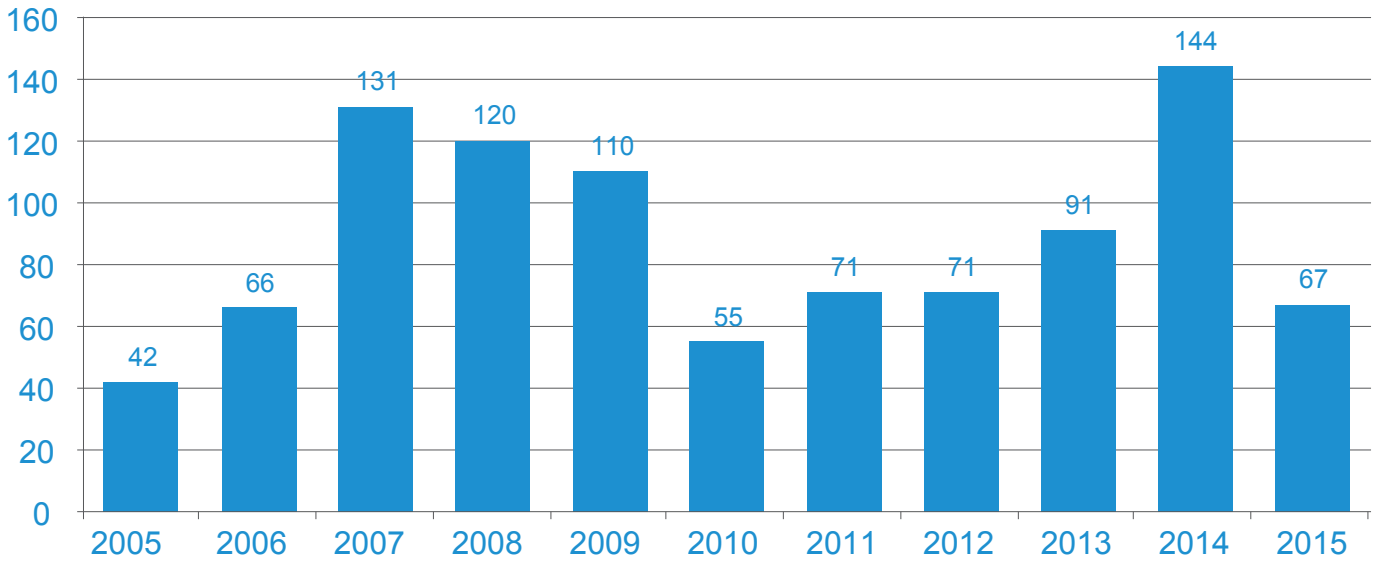


Fig. 2. Evolution of Prior Check Opinions issued by EDPS.

A large number (89% in 2015) of the risky processing operations notified to us relate to administrative procedures common to all EU institutions and bodies, such as the recruitment of staff, their annual evaluation or the conduct of administrative guidelines.

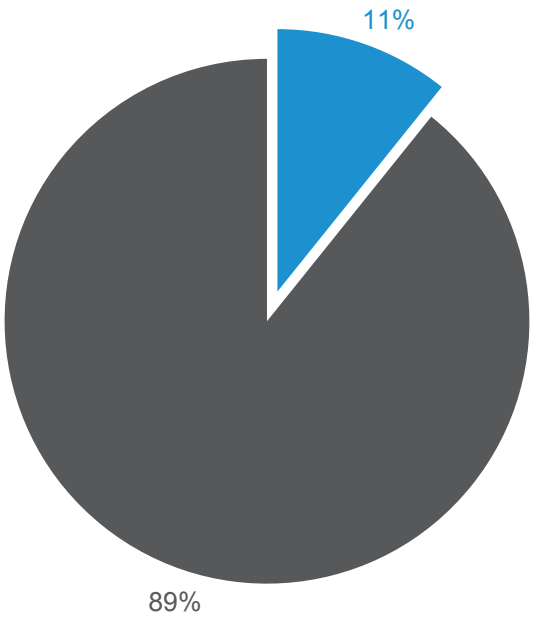


Fig. 3. Percentage split between Core Business and Administration activities in the Notifications received by EDPS.

Complaints

In 2015, the EDPS received 143 complaints, an increase of approximately 30% compared to 2014. Of these, 101 complaints were inadmissible, the majority relating to data processing at national level as opposed to processing by an EU institution or body.

The remaining 42 complaints required in-depth inquiry, an increase of about 8% compared to 2014. In addition, 31 admissible complaints, submitted in previous years (three in 2011, two in 2012, eight in 2013 and 18 in 2014), were still in the inquiry, review or follow-up phase on 31 December 2014. In 2015 we issued 18 complaint decisions.

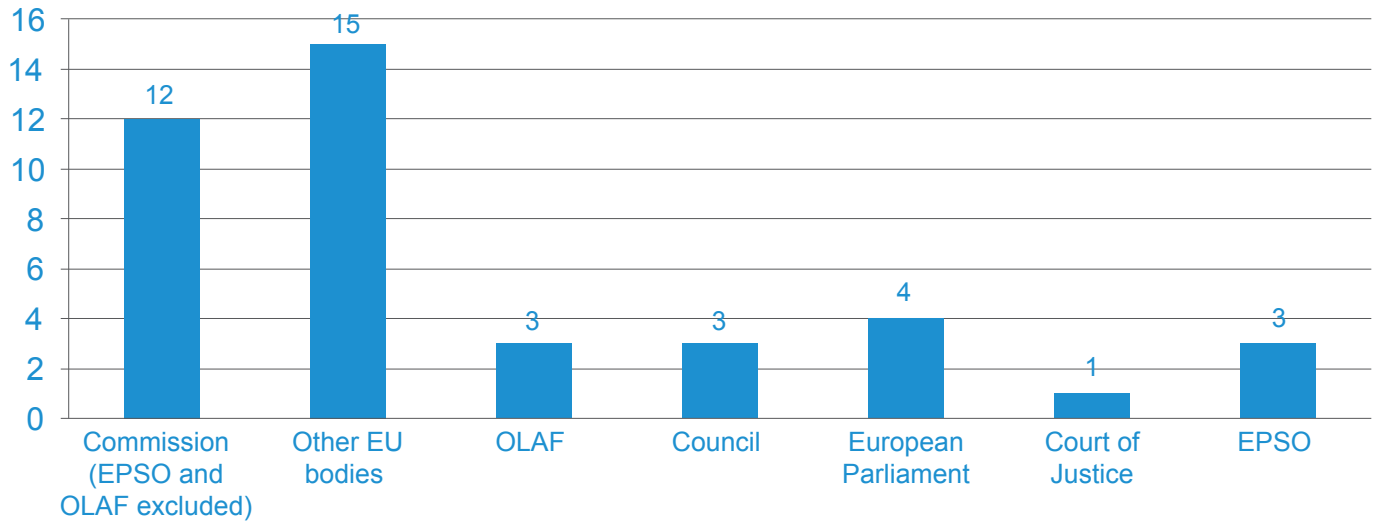


Fig. 4. Evolution of the number of complaints received by EDPS.

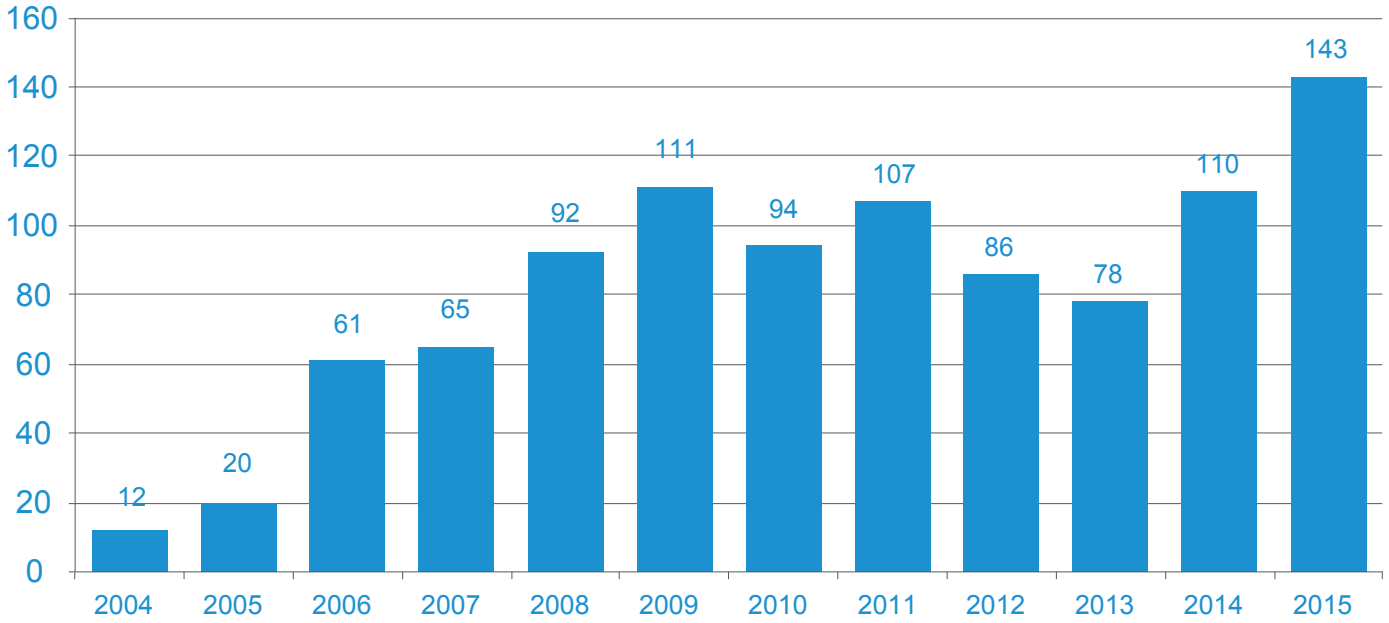


Fig. 5. EU institutions and bodies concerned by complaints received by EDPS

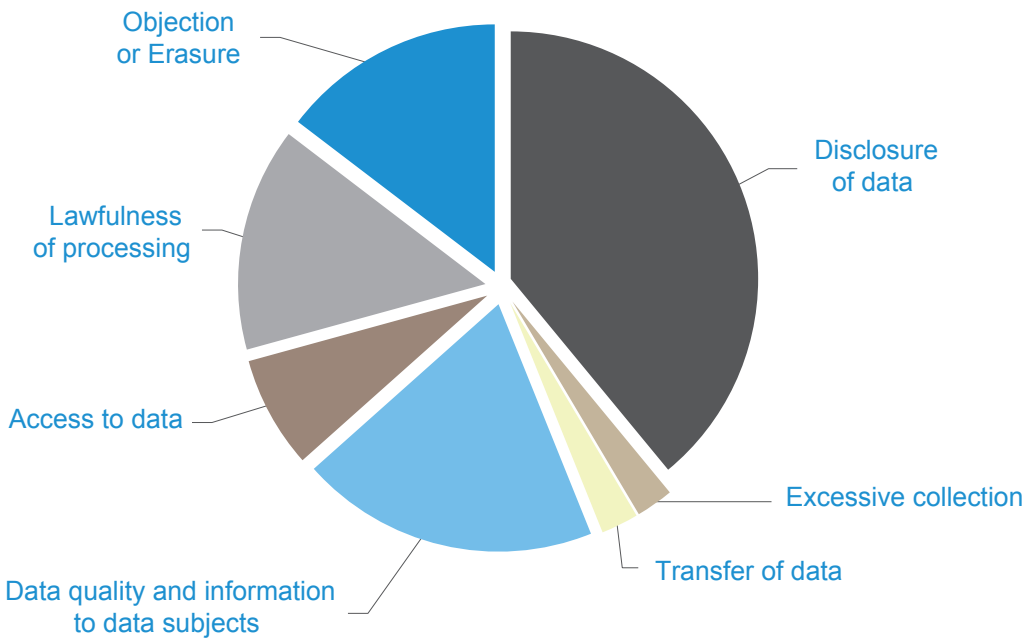


Fig. 6. Type of violation alleged in complaints received by EDPS.

Monitoring compliance

The EDPS is responsible for monitoring and ensuring the application of Regulation (EC) No 45/2001. Monitoring is primarily performed by bi-annual periodic general surveys; the results of the 2015 survey will be released in early 2016.

Visits

Between January and December 2015 we visited five EU agencies: the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU (Frontex), the European Union Agency for Network and Information Security (ENISA), the Office for Harmonisation in the Internal Market (OHIM), the European Securities and Markets Authority (ESMA).

Inspections

During the course of 2015, the EDPS undertook five inspections. These took place at the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), the Translation Centre for the Bodies of the European Union (CdT), the European Investment Bank (EIB), the European Commission (DG HR) and the European Union Visa Information System (VIS).

Consultations on administrative measures

In 2015, we received 52 consultations on administrative measures and issued 29 consultation opinions.

Annex D - List of Data Protection Officers

Council of the European Union	*Carmen LOPEZ RUIZ*
European Parliament	*Secondo SABBIONI*
European Commission	*Philippe RENAUDIERE*
Court of Justice of the European Union	*Sabine HACKSPIEL*
Court of Auditors	*Johan VAN DAMME*
European Economic and Social Committee (EESC)	*Lucas CAMARENA JANUZEC*
Committee of the Regions (CoR)	*Rastislav SPÁC*
European Investment Bank (EIB)	*Alberto SOUTO DE MIRANDA (DPO)* *Clare EVANS MCNALLY (Assistant DPO)*
European External Action Service (EEAS)	*Carine CLAEYS*
European Ombudsman	*Juliano FRANCO*
European Data Protection Supervisor (EDPS)	*Massimo ATTORESI*
European Central Bank (ECB)	*Barbara EGGL*
European Anti-Fraud Office (OLAF)	*Laraine LAUDATI*
Translation Centre for the Bodies of the European Union (CdT)	*Martin GARNIER*
Office for Harmonisation in the Internal Market (OHIM)	*Pedro DUARTE GUIMARÁES*
Agency for Fundamental Rights (FRA)	*Nikolaos FIKATAS*
Agency for the Cooperation of Energy Regulators (ACER)	*Appointment pending*
European Medicines Agency (EMEA)	*Alessandro SPINA*
Community Plant Variety Office (CPVO)	*Gerhard SCHUON*
European Training Foundation (ETF)	*Tiziana CICCARONE*
European Asylum Support Office (EASO)	*Luis CERDÁN ORTIZ-QUINTANA (DPO)* *Francesca MARCON (Assistant DPO)*
European Network and Information Security Agency (ENISA)	*Athena BOURKE (DPO)* *Ingrida TAURINA (Deputy DPO)*
European Foundation for the Improvement of Living and Working Conditions (Eurofound)	*Markus GRIMMEISEN*
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	*Ignacio VÁZQUEZ MOLINÍ*
European Food Safety Authority (EFSA)	*Claus REUNIS*
European Maritime Safety Agency (EMSA)	*Malgorzata NESTEROWICZ*
European Centre for the Development of Vocational Training (CEDEFOP)	*Spyros ANTONIOU* *Jesus BUSTAMANTE*
Education, Audiovisual and Culture Executive Agency (EACEA)	*Dirk HOMANN (DPO)* *Panagiota KALYVA (Assistant DPO)*

European Agency for Safety and Health at Work (EU-OSHA)	*Michaela SEIFERT*
European Fisheries Control Agency (EFCA)	*Rieke ARNDT*
European Union Satellite Centre (EUSC)	*Esther MOLINERO*
European Institute for Gender Equality (EIGE)	*Ramunas LUNSKUS*
European GNSS Supervisory Authority (GSA)	*Triinu VOLMER*
European Railway Agency (ERA)	*Zografia PYLORIDOU*
Consumers, Health and Food Executive Agency (Chafea)	*Despoina LEIVADINOU*
European Centre for Disease Prevention and Control (ECDC)	*Andrea IBER*
European Environment Agency (EEA)	*Olivier CORNU*
European Investment Fund (EIF)	*Jobst NEUSS*
European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)	*Andrzej GRAS*
European Securities and Markets Authority (ESMA)	*Sophie VUARLOT-DIGNAC (Acting DPO)* *Enrico GAGLIARDI (Deputy DPO)*
European Aviation Safety Agency (EASA)	*Francesca PAVESI (DPO)* *Milos PRVULOVIC (deputy DPO)*
Executive Agency for Small and Medium-sized Enterprises (EASME)	*Elke RIVIERE (DPO)* *Ana Elen Pallarés ALLUEVA (Deputy DPO)*
Innovation and Networks Executive Agency (INEA)	*Zsófia SZILVÁSSY*
European Banking Authority (EBA)	*Joseph MIFSUD*
European Chemicals Agency (ECHA)	*Bo BALDUYCK*
European Research Council Executive Agency (ERCEA)	*Giuseppe BAMBARA (Acting DPO)*
Research Executive Agency (REA)	*Evangelos TSAVALOPOULOS*
European Systemic Risk Board (ESRB)	*Barbara EGGL*
Fusion for Energy	*Angela BARDENHEWER-RATING*
SESAR Joint Undertaking	*Laura GOMEZ*
ECSEL	*Anne SALAÜN*
Clean Sky Joint Undertaking	*Bruno MASTANTUONO*
Innovative Medicines Initiative Joint Undertaking	*Estefania RIBEIRO*
Fuel Cells & Hydrogen Joint Undertaking	*Georgiana BUZNOSU*
European Insurance and Occupations Pensions Authority (EIOPA)	*Catherine COUCKE*
Collège européen de police (CEPOL)	*Leelo KILG-THORNLEY*
European Institute of Innovation and Technology (EIT)	*Jari AHOLA (Acting)*
European Defence Agency (EDA)	*Silvia POLIDORI*
Body of European Regulators for Electronic Communications (BEREC)	*Michele Marco CHIODI*
European Union Institute for Security Studies (EUISS)	*Nikolaos CHATZIMICHALAKIS*
eu-LISA	*Fernando DA SILVA*

Annex E - List of prior check and non-prior check opinions

Administration

Anti-fraud, whistleblowing and finance

- Restrictive Measures (Sanctions), European External Action Service (EEAS), 18 December 2015 (2014-0926)
- Reporting fraud and irregularities, European Medicines Agency (EMA), 16 December 2015 (2015-0820)
- External cases of potential fraud and/or other financial irregularities, Research Executive Agency (REA), 8 December 2015 (2013-1038)
- Whistleblowing, Committee of the Regions, 8 December 2015 (2015-0897)
- Whistleblowing, European Fisheries Control Agency (EFCA), 29 September 2015 (2015-0569)
- Whistleblowing, Council of the European Union, 15 September 2015 (2015-0349)
- Transactional Due Diligence, European Investment Fund, 10 July 2015 (2014-0758)
- Potential fraud and irregularities, European Research Council Executive Agency (ERCEA), 7 May 2015 (2015-0061)
- Exclusion Procedures, European Investment Bank, 19 March 2015 (2014-1110)

Administration and Human Resources

- Invalidity - Controls on invalidity persistence, European Parliament, 18 December 2015 (2014-0769)
- Stress screening test based on heart rate variability (Lifestyle Assessment), Committee of the Regions, 17 December 2015 (2015-0509)
- Growing Talent Training Programme, European Parliament, 27 November 2015 (2015-0636)
- Internal Mobility, European Chemicals Agency (ECHA), 20 October 2015 (2013-0573)
- Counselling Service, European Medicines Agency (EMA), 15 October 2015 (2013-0627)
- Staff Rotation Exercise in EU Delegations, European Commission, 6 October 2015 (2013-1092)
- Disciplinary Measures, European Union Satellite Centre (EU SatCen), 10 September 2015 (2014-0612)
- Allowances for staff members' disabled dependants, European Union Satellite Centre (EU SatCen), 10 September 2015 (2014-1095)
- Administrative Inquiries and Disciplinary Procedures, Body of European Regulators for Electronic Communications (BEREC), 23 July 2015 (2015-0532)
- Disability establishment and provision or reasonable accommodation, European Parliament, 22 July 2015 (2015-0366)
- Breach of trust, European Agency for Health and Safety at Work (EU-OSHA), 10 June 2015 (2015-0325)
- Career guidance and internal mobility, Committee of the Regions, 4 May 2015 (2013-0901)
- Flexitime and Leave, European Union Satellite Centre (EU SatCen), 10 April 2015 (2014-0605)
- Treatment of Medical Data, Court of Auditors, 1 April 2015 (2013-0810)
- Asbestosis Screening Programme, Court of Justice of the European Union, 25 March 2015 (2012-1091)
- Administrative enquiries and Disciplinary Procedures, Fusion for Energy Joint Undertaking (F4E), 4 March 2015 (2013-0808)

- Management of traineeship applications, European Institute for Security Studies (EUISS), 21 January 2015 (2014-0752)
- Invalidity Pension procedure, European Union Satellite Centre (EU SatCen), 21 January 2015 (2014-1093)
- Childcare facilities for children of employees, European Investment Bank, 12 January 2015 (2013-0585)

Anti-harassment

- Selection of Confidential Counsellors, European Agency for Health and Safety at Work (EU-OSHA), 7 September 2015, (2015-0562)
- Informal procedures for psychological and sexual harassment, European Agency for Health and Safety at Work (EU-OSHA), 28 July 2015 (2015-0467)
- Selection of Confidential Counsellors, European Environment Agency (EEA), 25 January 2015 (2013-0792)
- Selection of Confidential Counsellors, European Union Satellite Centre (EU SatCen), 30 January 2015 (2014-1117)

Evaluation (360° etc. and Staff Appraisal)

- Evaluation of Chair and Executive Director, European Insurance and Occupational Pensions Authority (EIOPA), 18 December 2015 (2015-0693)
- 360° feedback tool on leadership competencies, European Commission, 17 December 2015 (2015-0967)
- Appraisal, European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), 10 December 2015 (2015-0915)
- Peer Feedback Questionnaire, Office for Harmonisation in the Internal Market (OHIM), 24 November 2015 (2015-0733)
- 360° Feedback - Management Development Programmes (EPSO) (Joint opinion), European Commission, 15 October 2015 (2015-0737, 2015-0750)
- Probationary Period Procedure, European Union Satellite Centre (EU SatCen), 23 September 2015 (2014-1074)
- Probationary Period Reports for Management, Fusion for Energy Joint Undertaking (F4E), 22 September 2015 (2013-0727)
- 180° feedback tool on leadership competencies; 360° feedback exercise (Joint Opinion),European Commission, 16 July 2015 (2015-0440, 2015-0441)
- Evaluation, European Banking Authority, 23 April 2015 (2013-1064)
- SSM Performance Feedback, European Central Bank, 7 April 2015 (2015-0016)
- Appraisal, European Foundation for the Improvement of Living and Working Conditions (Eurofound), 13 March 2015 (2014-1011)
- 360° Feedback tool for managers, European Parliament, 12 March 2015 (2014-1146)
- Probation (Joint Opinion), European Central Bank, 12 January 2015 (2011-1105, 2011-1106, 2011-1107, 2014-0774)
- Evaluation and Probation, Electronic Components and Systems for European Leadership Joint Undertaking (ECSEL), 12 January 2015 (2013-0310)

Grants and Public Procurement

- Public procurement and Grant Procedures (Joint Opinion), Executive Agency for Small and Medium-sized Enterprises (EASME), 13 March 2015 (2013-0862, 2013-1050)
- Public procurement, European Insurance and Occupational Pensions Authority (EIOPA), 12 January 2015 (2013-0661)
- Public procurement, European Network and Information Security Agency (ENISA), 12 January 2015 (2011-1150)

Recruitment

- Open Selection procedure for Executive Director, European Insurance and Occupational Pensions Authority (EIOPA), 18 December 2015 (2015-0685)

- Selection Committee, European Insurance and Occupational Pensions Authority (EIOPA), 26 November 2015 (2015-0686)
- Recruitment, European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), 29 September 2015 (2015-0635)
- Pre-recruitment medical examination and annual medical check-up, European Union Satellite Centre (EU SatCen), 10 September 2015 (2014-1071)
- Recruitment of Trainees, European Union Satellite Centre (EU SatCen), 24 July 2015 (2014-1072)
- Recruitment of Local Staff, European Union Satellite Centre (EU SatCen), 24 July 2015 (2014-1082)
- Selection Procedure for Director of the European Union Agency for Fundamental Rights (FRA), European Parliament, 20 July 2015 (2015-0500)
- Update of Recruitment Procedures (Joint Opinion), European Commission, 7 July 2015 (2013-1275, 2013-1277, 2013-1278, 2013-1279, 2013-1280, 2013-1281, 2013-1282)
- Pre-selection procedure for the Director of the European Agency for Fundamental Rights (FRA), Council of the European Union, 30 June 2015 (2015-0463)
- Staff recruitment, European Police College (CEPOL), 1 June 2015 (2014-1103)
- Screening tool for Candidate Interpreters, European Parliament, 5 May 2015 (2015-0165)
- Recruitment of Seconded National Experts (Joint Opinion), European Union Satellite Centre (EU SatCen), 28 April 2015 (2014-0601, 2014-0602)
- Recruitment, European Asylum Support Office (EASO), 23 April 2015 (2014-1123)

Core Business

- Eurodac MSI/ Optical Scan Tests Study, European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), 25 November 2015 (2015-0082)
- Case Management Tool; Potential breaches of REMIT through the Notification Platform (Joint Opinion), Agency for the Cooperation of Energy Regulators (ACER), 2 October 2015 (2015-0545, 2015-0657)
- PeDRA - Personal data in Risk Analysis, European Agency for the Management of Operational Cooperation at the External Border (FRONTEX), 3 July 2015 (2015-0346)

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

Opinions

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

In 2015 the EDPS issued Opinions on the following subjects (date of publication in brackets):

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

Formal comments

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

In 2015 the EDPS issued formal comments on the following subjects (date of publication in brackets):

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

Annex G - Speeches by the Supervisor and Assistant Supervisor in 2015

European Parliament

Supervisor, Presentation of the EDPS 2014 Annual Report during the meeting of the Committee on Civil Liberties, Justice and Home Affairs, speech by Giovanni Buttarelli, European Parliament, Brussels (2 July 2015)

Supervisor, Trade agreements and data flows, speech given by Giovanni Buttarelli at the Joint Hearing of the INTA and LIBE committees, European Parliament, Brussels (16 June 2015)

Assistant Supervisor, Safeguarding Personal Data, Challenges and Opportunities of the shared economy, European Parliament, Brussels (1 June) [video from 1h39']

Supervisor, LIBE extraordinary meeting 26 February 2015: *Exchange of views with EDPS*, European Parliament, Brussels (26 February 2015)

Assistant Supervisor, Self-Regulation in the field of privacy, the EDPS point of view, seminar FEDMA Data & Privacy: Striking the Right Balance, European Parliament, Brussels (28 January 2015)

Supervisor, Counter-terrorism, De-Radicalisation and Foreign Fighters, speech by Giovanni Buttarelli given during the Joint debate at the extraordinary meeting of the LIBE Committee, European Parliament, Brussels (27 January 2015)

Supervisor, Privacy and Competition in the Digital Economy, speech by Giovanni Buttarelli given at the European Parliament´s Privacy Platform, Brussels (21 January 2015)

Council

Supervisor, A Data Protection perspective on the Smart Borders Package - focusing on the possibility of law enforcement authorities' access to border data, speech given by Giovanni Buttarelli at European Council, the Working Party on FRONTIERS, Brussels (19 November 2015)

European Commission

Assistant Supervisor, A Digital Strategy for Mobility: from capacity to connectivity, lecture during the conference on intelligent transport systems (ITS 2015), European Commission, DG MOVE, Brussels (24 April 2015)

Supervisor, Mentor Group Brussels Forum for EU-US Legal-Economic Affairs, Brussels (21 April 2015)

Other EU Institutions and bodies

Assistant Supervisor, Security, Privacy and the Industrial IoT during the seminar The Industrial Internet Era, organised by Politico Europe, Brussels (26 November 2015)

Supervisor, Hearing House of Lords Committee on Online Platforms and the EU DSM, Brussels (9 November 2015)

Supervisor, Competition Rebooted: Enforcement and personal data in digital markets, keynote speech given by Giovanni Buttarelli at Joint ERA-EDPS seminar (24 September 2015)

Assistant Supervisor, Data Protection in Non-Governmental Organisations, lecture during the data protection workshop organised by The European Fundraising Association, Brussels (25 June 2015)

Supervisor, EESC public hearing on Delegated acts, Brussels (26 May 2015)

Assistant Supervisor, Leading by Example: Data protection in the EU institutions, lecture in European School of Administration, Brussels (22 May 2015)

Supervisor, Big data, big data protection: challenges and innovative solutions, keynote speech by Giovanni Buttarelli given at ERA Conference on Recent Developments in Data Protection Law, Brussels (11 May 2015)

Supervisor, speech given at the Inter-institutional Informatics Committee at the Court of Justice, Luxembourg (23 February 2015)

International Conferences

Assistant Supervisor, Big Data Means Big Responsibility. Privacy Dimension of Knowledge Management Systems lecture during conference on Information and Value: Intellectual Property, Privacy and Big Data. International Conference on Intellectual Property and High Technology Law, Gdansk, Poland (20 November 2015) [Video]

Assistant Supervisor, Platform Services and Data Protection lecture during the conference Platform Services in the Digital Single Market, Osnabrück, Germany (19-20 November 2015)

Supervisor, 37th International Data Protection and Privacy Commissioners Conference, Amsterdam, The Netherlands (26 – 29 October 2015)

Assistant Supervisor, Data Stewardship for a 21st Century Data World: A Framework for Ethical Governance for Big Data Analytic Processing during 37th International Conference of Privacy and Data Protection Commissioners, Amsterdam, The Netherlands (26-29 October 2015)

Assistant Supervisor, Privacy perceptions of European consumers: The Symantec State of Privacy Report 2015 during 37th International Conference of Privacy and Data Protection Commissioners, Amsterdam, The Netherlands (26-29 October 2015)

Assistant Supervisor, Are we ready for the new model of cooperation under the GDPR? during I Workshop of PHAEDRA II Project (Improving practical and helpful cooperation between data protection authorities II), Amsterdam, The Netherlands (26-29 October 2015)

Assistant Supervisor, Protection of privacy and personal data is covered by the Data Protection Directive of 1995 lecture during the conference Freedom Not Fear 2015 Brussels (16-19 October 2015)

Supervisor, ENAM Conference Congress, EU Data Protection Regulation, Vilnius, Lithuania (16 October 2015)

Assistant Supervisor, Pros and Cons of the New Legal Framework for Data Protection lecture during the conference Biometrics 2015. Secure Identity Solutions Now, London, United Kingdom (13-15 October 2015)

Supervisor, Annual Privacy Forum 2015, Luxembourg, (7 October 2015)

Assistant Supervisor, Using employees and employee communication in social media as part of a corporate communication strategy during International Bar Association Annual Conference, Vienna, Austria (4-9 October 2015)

Assistant Supervisor, Security and Data Protection Friends or Foes lecture during the conference Free and Safe in Cyberspace. The role of new high-assurance IT paradigms and certifications in delivering constitutionally-meaningful privacy and security to all, while preserving public safety and cyber-investigation capabilities, Brussels (24-25 September 2015)

Assistant Supervisor, Noc architektów. Internet rzeczy - [Architects' Night. Internet of Things] during *XXI ICT Forum Moc danych – nowe źródła i nowe metody analizy i ochrony danych* organised in Warsaw, Poland (24-25 September 2015) [video]

Supervisor, 28th Annual International Conference Privacy Laws & Business, Cambridge, United Kingdom (6-7 July 2015)

Assistant Supervisor, Smart Data & Privacy by Design. Win-to-win business models on competitive digital market lecture during 18. International Conference Business Information Systems - BIS 2015 pt. *Making Big Data Smarter*, Poznan, Poland (24-26 June 2015)

Assistant Supervisor, The rocky road towards adoption of the new data protection regulation in 2015 and harmonisation of the 28 EU jurisdictions privacy frameworks during International Conference on Digital Privacy & Data Protection, Paris, France (2 June 2015)

Supervisor, The Digital Single Market, data protection and the role of the EDPS to 2020, speech given by Giovanni Buttarelli at Brussels Matters, Brussels (21 May 2015)

Supervisor, Spring Conference, Manchester, United Kingdom (19 May 2015)

Assistant Supervisor, Surveillance of the city and surveillance of citizens. Legal foundations of smart cities lecture during *VII Conference Internet Security Internet of Things. Security in the Smart City*, Warsaw, Poland (14-15 May 2015)

Assistant Supervisor, Why Will We Love Internet of Things and Why Should We Be Careful Being in Love lecture during The 6th Annual Internet of Things European Summit, Achieving Europe 2020 IoT role in building more inclusive, smarter and competitive Europe, Brussels (11-13 May 2015)

Assistant Supervisor, 26th IBA Annual Communications and Competition Conference organised by The International Bar Association, London, United Kingdom (11-12 May 2015)

Assistant Supervisor, Balancing Fundamental Rights – can it be done? organised in the scope of UK IAPP KnowledgeNet, London, United Kingdom (5 May 2015)

Assistant Supervisor, Is the Data Protection Law Technology Neutral lecture during 17th Meeting of Central and Eastern Europe Data Protection Authorities – CEEDPA – "Privacy and Technology: Challenges and Opportunities, Durrës, Albania (28-30 April 2015)

Assistant Supervisor, Forum on International Privacy Law organised by Cambridge Forum Inc., Cascais, Portugal (20-22 April 2015)

Assistant Supervisor, With Big Data Comes Big Responsibility – Emerging Corporate Best Practices to Enable Responsible Use of Big Data during the conference *IAPP Europe Data Protection Intensive, London*, United Kingdom (16 April 2015)

Assistant Supervisor, Leadership Beyond Digital. A Day For Leaders To Share, Learn and Prepare For A Challenging Future lecture during the Digital Forum seminar, Paris, France (14 April 2015)

Supervisor, Speech by Giovanni Buttarelli given at the Annual Dinner organised by the Center for Democracy and Technology, Washington D.C., United States (10 March 2015)

Supervisor, Washington Meetings Program and the Digital Cyberspace Policy Program: A Conversation with Giovanni Buttarelli, speech by Giovanni Buttarelli given at the Council on Foreign Relations, Washington D.C., United States (10 March 2015)

Supervisor, Data Protection Day event, *Respecting Privacy Safeguarding Data - Enabling Trust*, Brussels, (28 January 2015)

Supervisor, Concluding remarks delivered by Giovanni Buttarelli at the 8th CPDP Conference *Computers, Privacy & Data Protection - 2015 Data Protection on the Move*, Brussels (23 January 2015)

Other events

Supervisor, Data protection as a bulwark for digital democracy, keynote speech given by Giovanni Buttarelli at the 6th International e-Democracy 2015 Conference on Citizen rights in the world of the new computing paradigms, Athens, Greece (10 December 2015)

Supervisor, The General Data Protection Regulation: Making the world a better place?, keynote speech given by Giovanni Buttarelli at EU Data Protection 2015 Regulation Meets Innovation event, San Francisco, United States (8 December 2015)

Supervisor, Trust, Privacy and Security of Personal Data in the Digital World, keynote speech at Sofia, Bulgaria (18 November 2015)

Supervisor, Annual Data Forum-Politico, Brussels (17 November 2015)

Supervisor, Visit of the EDPS to the German DPAs, Representation of the State of Hessen, Berlin, Germany (16 November 2015)

Supervisor, Europe's big data protection opportunity, keynote address of Giovanni Buttarelli given at the Banking and Payments Federation, Ireland (8 October 2015)

Assistant Supervisor, Legal Grounds for Data Processing in the General Data Protection Regulation lecture during the conference, Nowe ramy ochrony danych osobowych w UE. Wyzwania dla Polski (New Data Protection Framework in EU. Challenges for Poland), Warsaw, Poland (18 September 2015)

Assistant Supervisor, Global Context of Data Protection lecture during the seminar Global Antitrust Hot Topics: EU, US & Global Perspectives, Brussels (17 September 2015)

Assistant Supervisor, Privacy and Personal Data Protection lecture in the scope of 3. ELSA Summer School Law of Information Technology, Brno, Czech Republic (2-9 August 2015)

Assistant Supervisor, Speaking notes from the speech of Wojciech Wiewiórowski on mHealth given at General Assembly of Association Internationale de la Mutualité, Liège, Belgium (23 June 2015)

Assistant Supervisor, Prywatność jako prawo podstawowe w Unii Europejskiej i w Konstytucji RP (*Privacy as the Fundamental Right in the European Union and in Polish Constitution*) lecture at Poland in Europe Academy, Wroclaw, Poland (12 June 2015)

Supervisor, Anti-fraud investigations and data protection in the EU, speech by Giovanni Buttarelli given at the European Anti-Fraud Congress, Brussels (5 June 2015)

Supervisor, II workshop of Internet Privacy Engineering Network, Leuven, Belgium (5 June 2015)

Assistant Supervisor, Engineering Privacy. The Role of IT Experts in Current development of the Data Protection Framework lecture during II workshop of Internet Privacy Engineering Network, Leuven, Belgium (5 June 2015)

Supervisor, Lecture KU Leuven, Belgium (21 May 2015)

Supervisor, Conference at the Italian Cassation Court on *Diritto all'identità personale e diritto all'oblio*, Rome, Italy (14 May 2015)

Assistant Supervisor, Personal data – local or global question on enlarging digital market, and Europejski Rynek Cyfrowy a gospodarka during conference Europejski Rynek Cyfrowy – umiejętności, gospodarka, praca, Warsaw, Poland (14 May 2015)

Supervisor, International Data Exports - EU-US Data Transfers, Brussels (7 May 2015)

Supervisor, Speech given by Giovanni Buttarelli at the Vienna Parliamentary Forum on Intelligence-Security, Vienna, Austria (6 May 2015)

Supervisor, Value of the EU data protection reform against the big data challenges, keynote address by Giovanni Buttarelli given at the 5th European Data Protection Days, Berlin, Germany (4 May 2015)

Supervisor, Keynote address by Giovanni Buttarelli given at the Cybersecurity and Privacy Innovation Forum 2015, Brussels (28 April 2015)

Assistant Supervisor, The role of national legislation at the time of the revision of European Union rules on data protection, lecture during conference Ochrona danych osobowych po zmianach wprowadzonych nowelizacją z 7.11.2014 r., Warsaw, Poland (23 March 2015)

Assistant Supervisor, How the universities teach the students to be ready to work in European institutions, lecture for the participants of the study visit by Pomeranian universities and scientific centres by Regional Bureau of Pomeranian Voivodship, Brussels (4-6 March 2015)

Supervisor, EDPS Strategy 2015-2019, speech by Giovanni Buttarelli given at the occasion of the presentation of the EDPS Strategy 2015-2019, Brussels (2 March 2015)

Supervisor, Libertà, responsabilità ed etica: nuove sfide per la tutela della web generation, Milan, Italy, Videoconference (9 February 2015)

Supervisor, Antitrust, Privacy and Big Data, speaking points of Giovanni Buttarelli for a seminar on competition, privacy and big data, Brussels (3 February 2015)

Assistant Supervisor, Users' Control Over Their Data: Is Prior Consent the Best Way to Monitor, during the conference Computers, Privacy and Data Protection (CPDP), Brussels (21-23 January 2015)

Supervisor, Big data, big challenges, article by Giovanni Buttarelli for New Europe (5 January 2015)

Annex H - Composition of EDPS Secretariat

Director, Head of Secretariat

Christopher DOCKSEY

Christian D'CUNHA
Policy Assistant to the EDPS

Hielke HIJMANS
Special Adviser

Daniela OTTAVI
Planning/Internal Control Coordinator

Supervision and Enforcement

Maria Verónica PEREZ ASINARI
Head of Unit

Isabelle Chatelier
Head of Complaints and Litigation

Delphine HAROU
Head of Prior Checks and Consultation

Ute KALLENBERGER
Head of Inspections

Stephen ANDREWS
Supervision and Enforcement Assistant

Petra CANDELLIER
Legal Officer

Mario GUGLIELMETTI
Legal Officer

Xanthi KAPSOSIDERI
Legal Officer

Owe LANGFELDT
Legal Officer

Anna LARSSON STATTIN
Legal Officer/Seconded National Expert

Bénédicte RAEVENS
Legal Officer

Snezana SRDIC
Legal Officer

Tereza STRUNCOVA
Legal Officer

Policy and Consultation

Sophie LOUVEAUX
Head of Unit

Anne-Christine LACOSTE
Head of International Cooperation

Anna BUCHTA
Head of Litigation and Institutional Policy

Alba BOSCH MOLINE
Legal Officer

Zsuzsanna BELENYESSY
Legal Officer

Gabriel Cristian BLAJ
Legal Officer

Elena JENARO*
Legal Officer
Assistant Data Protection Officer

Amanda JOYCE
Policy and Consultation Assistant

Jacob KORNBECK
Legal Officer

Romain ROBERT
Legal Officer

Fabio POLVERINO
Legal Officer

Lara SMIT
Legal Officer

Evelien VAN BEEK
Legal Officer

Gabriela ZANFIR
Legal Officer

IT Policy

Achim KLABUNDE
Head of Sector

Luisa PALLA
Head of Records Management

Massimo ATTORESI
Technology and Security Officer
Data Protection Officer

Andy GOLDSTEIN
Technology and Security Officer
LISO

Malgorzata LAKSANDER
Technology and Security Officer

Fredrik LINDHOLM
Administrative Assistant

Fidel SANTIAGO
Technology and Security Officer

Records Management Group

Marta CORDOBA-HERNANDEZ
Administrative Assistant

Kim Thien LÊ
Administrative Assistant

Séverine NUYTEN
Administrative Assistant

Carolina POZO LOPEZ
Administrative Assistant

Maria Jose SALAS MORENO
Administrative Assistant

Martine VERMAUT
Administrative Assistant

Information and Communication

Olivier ROSSIGNOL
Head of Sector

Thomas HUBERT
Graphic Designer Assistant

Courtenay MITCHELL
Information and Communication Officer

Parminder MUDHAR
Information and Communication Officer

Agnieszka NYKA
Information and Communication Officer

Benoît PIRONET
Web Developer

Human Resources, Budget and Administration

Leonardo CERVERA NAVAS
Head of Unit

Sylvie PICARD
Head of HR Coordination and Planning

Maria SANCHEZ LOPEZ
Head of Finance

Claudia BEATO
HR Assistant

Pascale BEECKMANS
HR Assistant
GEMI

Laetitia BOUAZZA-ALVAREZ
HR Assistant
GECO
LSO
Traineeship Coordinator

Vittorio MASTROJENI
Human Resources Officer

Julia MOLERO MALDONADO
Finance Assistant

Anne-Françoise REYNDERS
Human Resources Officer
L&D Coordinator

Caroline WOUSSEN
Finance Assistant

** staff members who left the EDPS in the course of 2015*

Publications Office

www.edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

EDPS

European Data Protection Supervisor