ISSN 1830-9585

European Data Protection Supervisor

Annual Report 2014

EDPS

European Data Protection Supervisor

An Executive Summary of this Report which gives an overview of key developments in EDPS activities in 2014 is also available.

Hard copies of the Annual Report and the Executive Summary may be ordered free of charge from the EU Bookshop (http://www.bookshop.europa.eu).

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.

@EU_EDPS

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, 2015

Print	ISBN 978-92-9242-067-3	ISSN 1830-5474	doi:10.2804/215329	QT-AA-15-001-EN-C
PDF	ISBN 978-92-9242-065-9	ISSN 1830-9585	doi:10.2804/129707	QT-AA-15-001-EN-N
EPUB	ISBN 978-92-9242-066-6	ISSN 1830-9585	doi:10.2804/72275	QT-AA-15-001-EN-E

Printed in Italy
PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

Annual Report 2014

Contents

MISSION STATEMENT, VALUES AND PRINCIPLES

The European Data Protection Supervisor (EDPS) is the European Union's independent data protection authority established under Regulation (EC) No. 45/2001 (henceforth the Regulation),[1] 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 development 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.

1 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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 (OJ L 8, 12.1.2001, p. 1).

FOREWORD

In recent years, data protection has moved from the margins to the centre ground of political decision making and business planning.

For the EU, 2014 may be remembered in future years as a watershed, the moment the rights to privacy and to the protection of personal data as set down in the Charter of Fundamental Rights moved decisively from legal theory to reality. The European Court of Justice, in its landmark judgments on the Data Retention Directive and Google Spain, articulated the responsibility of lawmakers and controllers for ensuring personal information is processed fairly and in a manner proportionate to the legitimate purpose being pursued. Deliberations on the reform of the EU's rulebook, which are now in their fourth year, edged closer to a conclusion, with the European Parliament giving a resounding endorsement to a revised text of the General Data Protection Regulation, and the Council grappling with the crucial questions of enforcement and consistency. Meanwhile, concerns about mass surveillance deepened, with the growing realisation of the need to revise and to clarify the parameters for data flows between the EU and its global partners.

2014 was a year of transition for the EU in general, as well as for our own institution. This Annual Report reviews the activities of the European Data Protection Supervisor and our focus on increasing the capacity of EU bodies for accountable data processing and for more proactive integration of data protection rules and principles in policy making. In addition to prior checks of processing operations and inspections, and numerous Opinions and comments on policy initiatives, including comments on the ongoing data protection reform, we have published several key guidance documents addressing, for example, data subjects rights, data transfers and data protection in financial services regulation.

This establishment of data protection in the mainstream of EU policymaking is a tribute to the calm authority and tireless efforts of Peter Hustinx, whose 10-year tenure as a European Data Protection Supervisor drew to a close in 2014, and to the talents and commitment of the people who work for this institution. Building on Peter's legacy, our priorities for the next five years, as set out in our Strategy published in March 2015, is to work more closely than ever with national data protection authorities as well as the Parliament and Member States, so that the EU speaks with one voice, credible and consistent, to uphold the rights and interests of the individual in our ever more globalised and digitalised society.

Giovanni Buttarelli
European Data Protection Supervisor

Wojciech Wiewiórowski
Assistant Supervisor

1. 2014 HIGHLIGHTS

1.1. General overview of 2014

2014 was a year of transition for the EDPS, marked by the delayed selection and appointment of a new Supervisor and Assistant EDPS. The nominations that had been expected at the beginning of the year took place only at the end. While the resulting uncertainty had an impact on the planning of activities of the EDPS as a whole, we continued to perform our duties in line with our obligations under Regulation (EC) 45/2001.

Supervision & Enforcement

In 2014, we continued to work closely with the DPOs appointed in the EU institutions, underlying their key role in ensuring compliance with the Regulation.

We continued to focus on awareness raising and guidance to help promote a data protection culture in the EU institutions. Of particular note were:

- the Rights of Individuals (Data Subjects Rights) Guidelines adopted in February, the Data Transfer Position Paper adopted in July and the Conflicts of Interest Guidelines adopted in December;
- several meetings with controllers to better understand the EU administration's constraints;
- three conferences at the European School of Administration (EUSA) and one workshop for Data Protection Coordinators;
- two DPO meetings in June and November.

Prior checking of processing operations likely to present specific risks continued to represent an important part of our work.

The number of complaints we received continued to increase in 2014, although the majority of these were inadmissible as they related to processing at national level as opposed to processing by an EU institution or body.

In line with our policy on consultations in the field of supervision and enforcement, EU institutions should first seek the advice of their own DPO and therefore involve them when drawing up measures affecting the right to data protection.

We continued to visit EU agencies that showed a lack of commitment to data protection and introduced consultancy visits by members of EDPS staff. In addition, we carried out inspections in line with our inspection plan.

In particular we carried out:

- two thematic targeted inspections on health data (one at the Council and one at the Commission covering 47 agencies) and a general inspections at the European Parliament. In addition, there was an inspection at FRONTEX, which was not in the initial planning;
- four visits: the EIB, GNSS Supervisory Authority, EUISS and the EU SatCen.

Policy and consultation

Where an initiative raises significant questions of compliance with data protection rules and

principles, be it a formal Commission proposal for a legal act or a communication setting out policy orientations, we issue Opinions which analyse these implications in depth. In 2014, we published 14 such Opinions.

We also issued a 'preliminary Opinion', on the interplay between competition, consumer and data protection law in the digital economy. The Opinion addressed the general topic from the perspective of the increasing importance of data protection.

We issued more limited advice, or formal comments, on 13 policy initiatives, in most cases within two months after the adoption of the document in question.

In 2014, we provided informal comments on 33 separate draft initiatives.

More proactive policy advice

In 2014, we reviewed how we fulfil the legal obligation to advise the institutions. In our June policy paper, 'The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience'[2], we reiterated our principles of impartiality, integrity, transparency and pragmatism and our broad, inclusive and proactive engagement with stakeholders. We aim to develop a culture of accountability across all EU institutions and bodies through training, and general as well as sector specific guidance to enable the institutions to make informed decisions on the data protection impacts of new proposals. We have already begun to target engagement with less familiar interlocutors who are increasingly aware of the relevance of data protection. In addition, we have established regular liaison and information sharing with the Fundamental Rights Agency (FRA) and international bodies including the Council of Europe.

On the basis of constructive and targeted dialogue with the institutions, we specifically undertook to develop a 'policy toolkit' – including thematic or sectoral guidelines – for guiding policy and law makers.

In November 2014, we delivered the first of these tools focusing on financial services regulation. Our sector guidelines built on insights gained during a seminar hosted by DG MARKT in February 2014.

With regard to specific initiatives, our 2014 'inventory' anticipated five key areas of strategic importance for data protection:

- Towards a new legal framework for data protection

2 EDPS Policy Paper, 'The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience', 4 June 2014.

- Rebuilding trust in global data flows in the aftermath of PRISM
- Initiatives to boost economic growth and the Digital Agenda
- Further developing the area of freedom, security and justice
- Reform of the financial sector.

Towards a new legal framework for data protection: An end in sight?

Reforming the data protection framework has constituted one of the largest and most complex challenges for EU lawmakers in recent years. There is great interest at national, European and international level in the evolution of the two draft proposals. The EDPS continued to work closely with the Parliament, the Council and the Commission during the critical discussions which took place in 2014.

Cooperation

In the area of cooperation, we continued to contribute actively to the work of the Article 29 Data Protection Working Party (Article 29 Working Party), also acting as rapporteur for the follow-up of the Opinion on Legitimate Interests (consultation of stakeholders and analysis of their contributions), and co-rapporteurs for the Opinion and the Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes, as well as for the paper on the International Enforcement Coordination Arrangement.

Court cases

With regard to Court activities we were granted leave to intervene by the Court of Justice and submitted a written statement in an appeal Case C-615/13 P, brought by ClientEarth and PAN Europe), a case related to transparency/access to documents.

Monitoring and reporting on technological development

In 2014, we strived to ameliorate our continuous monitoring of technological developments, events and incidents and the assessment of their impact on data protection. The impact of the wider spread of connected mobile devices and a high number of security incidents were among the themes of the year.

In order to ensure full compliance with data protection principles combined with effective and efficient solutions, we adopted the EDPS IT security policy in March.

A visit to eu-LISA headquarters served to improve the working relationship with the agency and to collect information for the preparation of future audits and inspections.

The number of serious security flaws discovered in widespread systems is increasing: in 2014, it was found that some of the most popular mobile devices were vulnerable to interception of seemingly encrypted communications. It was also revealed that a piece of code found in many Linux systems had a flaw allowing attackers to bypass security protections. A vulnerability was also discovered in smartphone operating systems.

In 2014, a number of security flaws in widely used systems attracted a lot of attention. Some of the vulnerabilities were given names like Heartbleed, Gotofail and Poodle. The Heartbleed bug[3] was discovered in OpenSSL, a popular encryption tool for internet communications. Heartbleed makes it possible to read and access data that should be protected.

Many popular internet services seemed to be vulnerable and appeared to take the necessary measures to quickly fix the bug on their systems. Users of affected services were advised to change their passwords and the certificates used for encrypting internet traffic between affected websites were replaced.

IT Policy Laboratory

The EDPS IT Policy Laboratory was set up in 2014 with equipment and tools that can be used to assess the privacy features of certain products or systems used in the field of our supervision work.

The IT lab is now operational and will be complemented by a mobile IT kit, in order to provide on-the-spot demonstrations, perform experiments and/or technical tests on-site during inspections and audits.

The IPEN initiative

An important action point in the new EDPS strategy is the promotion of privacy friendly technology through cooperation with different stakeholders.

In 2014, we launched the Internet Privacy Engineering Network (IPEN) in collaboration with national data protection authorities (DPAs), developers and researchers from industry and academia and civil society. The initiative aims to develop engineering practices which incorporate privacy concerns and

encourage engineers to build privacy mechanisms into internet standards, services and apps.

The first IPEN workshop took place on 26 September 2014 in Berlin. The workshop was designed to be a practical approach to identify privacy gaps in existing technology and develop useful solutions.

The theme of our debate was 'How can we develop internet services and apps which respect users' privacy and personal data?'

Among the projects proposed was the creation of a 'data protection cookbook' for system development. Participants also recommended the creation of a 'business process design cookbook', to provide guidance to businesses to integrate data protection in their ways of working.

Information & Communication

Information and communication activities play a significant role in raising awareness of the EDPS, the mandate, policies and decisions. Our activities target the EU administration and the wider public and we continued to use tools and activities such as press releases, publications, events, tweets and updates to our website. Our audiences have varying degrees of knowledge on the topic of data protection and we therefore tailor our approach to their differing needs.

In 2014, we promoted the work of the EDPS at a number of events, such as Data Protection Day in January, the EU Open Day in May and four lunch time conferences at the European School of Administration (EUSA).

Within the scope of our competence, we replied to 132 written information requests from citizens, 38 written information requests and 42 interview requests from the press.

By the end of 2014, we had 2373 subscribers to our newsletter and 2000 Twitter followers. We had

3 CVE-2014-0160.

194,637 visits to the EDPS website and we hosted seven study visits on our premises. These achievements all support the view that we are increasingly a point of reference for data protection issues at EU level.

Resource Management

The allocated budget for the EDPS in 2014 was EUR 8 018 796, which is an increase of 4.66% on the 2013 budget.

In 2014, we remained fully committed to the EU's policy of austerity and budget consolidation, and followed the orientations proposed by the Commission strictly. Nevertheless, our budget proposal had to include the necessary appropriations to comply with the statutory obligations linked to the end of mandate of the members of the EDPS.

We implemented the austerity policy recommended by the Commission by reducing or freezing a large majority of our credits to 0% for the third year and carrying out substantial cuts to key budget lines such as translations (-17%), publications (-25%) and activities of the institutions (-17%).

The delay in the selection procedure for a new team of Supervisors led to the introduction of an amending budget to return the unused credits linked to temporary extension of the mandate to the general EU budget in June 2014.

In 2014, the implementation rate of our budget exceeded the target of 85%.

2014 was a particularly successful year in the human resources area. The entry into force of the new Staff Regulations in January 2014 required many implementing measures to be updated. The full package of implementing rules was adopted before the end of the year.

A number of important policy documents were also adopted, notably the new Learning and Development policy and its implementation, two pilot projects and the papers on DNA, Stress and Internal Communication. In addition, a new Code of Conduct for EDPS Staff was adopted and presented to the Staff.

1.2. Strategy 2013-2014

In our Strategy 2013-2014, we identified a number of strategic objectives to help increase the impact of our core activities on data protection at European level. To assess our progress towards these objectives, we identified the activities which play a key role in achieving our goals. The related key performance indicators (KPIs) listed in the table help us to monitor and adjust, if needed, the impact of our work and the efficiency of our use of resources.

In this chapter, we report on the performance of our activities in 2014 in accordance with the strategic objectives and action plan defined in the Strategy 2013-2014. The activities implementing the action plan are summarised in the General Overview of 2014, above.

Overall, the results show a positive trend in the performance of our activities. The implementation of

Key EDPS figures in 2014

- ➔ **144 prior-check Opinions adopted, 26 non-prior check Opinions**
- ➔ **110 complaints received, 39 admissible**
- ➔ **48 consultations received on administrative measures**
- ➔ **4 on-the-spot inspections and 4 visits carried out**
- ➔ **2 sets of Guidelines published, 1 Position Paper**
- ➔ **14 legislative Opinions and 1 Preliminary Opinion issued**
- ➔ **13 sets of formal comments issued**
- ➔ **33 sets of informal comments issued**

the strategy is broadly on track and no corrective measures are needed at this stage.

In addition, the adoption of the Strategy 2015-2019 in March 2015 will require an evaluation of the KPIs to take into account the objectives and priorities of the new Strategy. As a result, to ensure their consistency and relevance, there may be one or more new KPIs, which will be submitted to thorough internal consultation before being published.

The KPI scoreboard contains a brief description of the KPIs and the methods of calculation.

The indicators are measured against initial targets in most cases. For three indicators, the results of 2013 set the benchmark for 2014.

The KPIs implement the strategic objectives as follows:

1. Promote a *data protection culture* within the EU institutions and bodies whereby they are aware of their obligations and accountable for compliance with data protection requirements.
   KPIs numbers 1, 2 and 3. All targets have been achieved.

2. Ensure that the EU legislator (Commission, Parliament and Council) is aware of data protection requirements and that data protection is integrated in new legislation.
   KPIs numbers 4 and 5. The target for KPI number 5 has been achieved. The results for KPI number 4 are in line with 2013 results with regard to formal and informal comments, while the number of opinions decreased in 2014. This was due, on the one hand, to a greater level of selectiveness and on the other to the fact that several Commission initiatives which we had identified were either deleted or delayed by the Commission (for instance, TAXUD negotiations with WTO and Russia).

3. Improve the good cooperation with data protection authorities (DPAs), in particular the WP29, to ensure greater consistency of data protection in the EU.
   The results of 2013 determine the target for KPI number 6. The results in 2014 were a great success, as they largely exceeded the target.
   KPI number 7 refers to strategic objectives 1, 2 and 3. The target was largely exceeded.

4. Develop an effective communication strategy.
   The results of 2013 determine the target for KPI number 8. In this respect the number of visits to the EDPS website decreased during 2014. The main reason was the delayed appointment of the new Supervisors. During the one-year extension of the mandate there were fewer new decisions or new projects. This had an impact on the interest to visit our website.

5. Improve the use of the EDPS' human, financial, technical and organisational resources (through adequate processes, authority and knowledge).
   KPIs numbers 9 and 10. Both targets have been achieved.

KPIs	Description	Results 2013	Results 2014	Target
KPI 1	Number of inspections/visits carried out Measurement: compared to target	3 visits 8 inspections	4 visits 4 inspections	8 minimum
KPI 2	Number of awareness-raising and training initiatives within EU institutions and bodies which we have organised or co-organised (workshops, meetings, conferences, training and seminars). Measurement: compared to target	4 trainings 4 workshop (3 in cooperation with ITP)	8 (3 EUSA, 1 DPC, 2 DPO, 1 EIPA, 1 DG COMM)	8 (workshops + trainings)
KPI 3	Level of satisfaction of DPOs/DPCs on training and guidance. Measurement: DPOs/DPCs satisfaction survey to be launched every time a training is organised or a guidance is issued	DPO basic training: 70% positive feedback EDA staff training: 92% positive feedback	100%	60% positive feedback
KPI 4	Number of EDPS formal and informal Opinions provided to the legislator. Measurement: compared to previous year	Opinions: 20 Formal comments: 13 Informal comments: 33	Opinions: 15 Formal comments: 13 Informal comments: 33	2013 as benchmark
KPI 5	Rate of implementation of cases in our policy inventory which we have identified for action. Measurement: percentage of 'Red' initiatives (where the dead-line for comments has expired) implemented as planned in the Inventory 2013	90% (18/20)	89%	90%
KPI 6	Number of cases dealt with by the Article 29 Working Party for which the EDPS has provided a substantial written contribution. Measurement: compared to previous year	13	27	2013 as benchmark
KPI 7	Number of cases in which guidance is provided on technological developments. Measurement: compared to target	21	58	20
KPI 8	Number of visits to the EDPS website. Measurement: compared to previous year	293.029 (+63% in comparison to 2012)	194.637	2013 as benchmark
KPI 9	Rate of budget implementation Measurement: amount of payments processed during the year divided by the budget of the year.	84,7%	85,8%	85%
KPI 10	Rate of training implementation for EDPS staff Measurement: number of actual training days divided by the number of estimated training days	85%	87,4%	80%

2. SUPERVISION AND ENFORCEMENT

Our strategic objective

Promote a *data protection culture* within the EU institutions and bodies so that they are aware of their obligations and accountable for compliance with data protection requirements.

2.1. Introduction

The task of the EDPS in his independent supervisory capacity is to monitor the processing of personal information carried out by EU institutions or bodies (except the Court of Justice acting in its judicial capacity). Regulation (EC) No 45/2001 (the Regulation) describes and grants a number of duties and powers, which enable the EDPS to carry out this task.

Public authorities must be beyond reproach on how they process personal information; the aim of our supervision work is to help them become exemplary.

Our supervision work aims to ensure that the more than 60 EU institutions and bodies process personal information fairly and lawfully. As any employer of over 40,000 members of staff, EU institutions and bodies develop administrative procedures necessary for effective management and smooth functioning. Their procedures include evaluation and promotion of staff, access control to their buildings, working hours of employees, policies to prevent sexual and psychological harassment, managing electronic communications and mobile devices. The functioning of any public administration also includes the relationship with citizens for instance, through access to documents requests, petitions or procurements. Outside the employment context, EU institutions and bodies also process personal information in various domains and for a wide range of purposes. Their core business activities reflect the issues of European society; from food safety to disease prevention and financial stability.

As a supervisory authority, we systematically scrutinise risky procedures adopted by the EU institutions and bodies in line with our prior checking obligation. We investigate complaints and reply to questions related to data protection matters. We have dealings with the Court of Justice of the European Union where EDPS decisions in complaint cases can be appealed before the Court (the EDPS can also refer a matter to the Court, as well as intervene in actions before the Court, see chapter 5).

We also supervise the central units of a number of large-scale IT systems for matters such as asylum, visas and customs cooperation. Among other things, we respond to consultations and conduct inspections. As supervisor of the central units, we also participate in the supervision coordination groups (see chapter 4) as a member on equal footing with national DPAs.

Over the years, we have developed considerable expertise on data protection not only in the context of employment but in other areas such as selection of experts, asset freezing and transfers of personal data outside the EU. As a result, we are able to share the advice resulting from this expertise with the EU institutions and the larger public for instance, through the thematic guidelines that we publish.

We also examine the use of new technologies that have an impact on data protection such as cloud computing and provide advice and recommendations on how to minimise their impact on individuals' rights and freedoms. This experience of analysing big data processes, such as transfers of data, in the institutions has helped us to tailor our advice so that data protection helps the institutions comply with the law, rather than hinder the process.

We use our expertise and authority to supervise the EU institutions and bodies in an independent manner in accordance with our policy adopted in December 2010. Independence is an essential element to conduct our mission but independent supervision does not mean that we are isolated from our EU partners. We strongly believe in and value our cooperation with our data protection partners, the data protection officers (DPOs) and data protection coordinators (DPCs). We support

them and rely on them to act as a relay. Our support for DPOs and DPCs takes on different forms: we continuously provide training and guidance, we visit institutions to remind management that it is their duty to cooperate with the DPOs, we offer on the spot consultations and we have opened informal communication channels to reduce the burden of bureaucracy.

Cooperation also means that we adapt to the specific context of each EU institution and body and offer pragmatic solutions so that our advice is relevant. We promote direct interaction with institutions through meetings and conference calls.

We seek to ensure compliance through persuasion and example but we do not hesitate to use our enforcement powers when necessary. We focus our efforts where the impact on privacy and data protection are greatest.

We believe in accountability mechanisms that facilitate the compliance process and therefore we help EU institutions to take responsibility for processing personal information. Our activities aim to encourage the commitment of senior and middle management.

While EDPS advice has been developed for the EU institutions and bodies, the scale and scope of our supervision work means that this advice may be valuable for others, for example, public sector bodies and international organisations as general guidance on fundamental rights.

2.2. Data Protection Officers

Under Article 24.1 of the Regulation, European Union institutions and bodies each have an obligation to appoint at least one data protection officer (DPO). The EDPS considers that the DPOs are key to any successful accountability programme. We have therefore developed a number of activities and tools aiming to provide support to DPOs in the performance of their work. These include a dedicated DPO corner on the EDPS website, a telephone helpline and specific DPO training. The EDPS also participates in the biannual DPO network meetings.

In 2014, we received notifications for the appointment of 9 new DPOs in the EU institutions.

For a number of years, the DPOs have met at regular intervals in order to share common experiences and discuss horizontal issues. This informal network, which has proved to be productive and encourages collaboration, continued throughout 2014. We continued to work closely with the DPO quartet which was established to coordinate the DPO network.

We attended the DPO meeting held in Brussels in June (hosted by the European Parliament and the European Commission) and in Thessaloniki (hosted by the European Centre for the Development of Vocational Training, Cedefop) in November.

At the June meeting, we presented an update on the EU reform of the data protection legislation and relevant case law in the area. The meeting was also an appropriate opportunity for us to present our guidelines on data subject rights which led to an in-depth discussion on how to address such requests in practice.

The meeting at Cedefop was an occasion to reflect on the new EDPS mandate and the role of DPOs in the international scene. We also presented our position paper on transfers which was adopted in July 2014 and our guidelines on conflicts of interests, both of which gave rise to interesting debates. Also well appreciated was our update on security and technology issues with particular reference to the EDPS experience of using the cloud and security breach handling. We also presented some notable issues dealt with in our Supervision and Enforcement work such as the procedure for consultations at the CCA (Collège des Chefs d'administration), the involvement of DPOs in complaint handling and the importance of documenting deferral of rights in accordance with Article 20 of the Regulation.

The DPO meetings have clearly demonstrated the need for longer exchanges between the EDPS and the DPOs on the complex challenges some DPOs face in the implementation of the Regulation. An invitation to discuss the format of the DPO meetings with the EDPS was therefore extended with a view to allow more time for interaction.

In June 2014, we organised a training session for DPOs back-to-back with the DPO meeting (see section 2.7 Data Protection Guidance). In addition, one-to-one sessions took place between EDPS staff and some DPOs on their specific guidance needs. The development of consultancy visits (see section 2.5) has also served to address the specific needs of DPOs.

In the course of our Supervision and Enforcement work, we also field telephone queries posed by

DPOs and whenever possible provide immediate assistance and guidance on specific issues, while dealing with more complex ones in written consultations (see section 2.6 Consultations on administrative measures). In response to the increasing number of telephone queries we receive, we set up a helpline for DPOs, operational at set times in the week and answered by an EDPS member of staff. The helpline allows us to provide specific guidance on simple questions from DPOs in a quick and informal way and strengthens the good cooperation and communication between us and the DPO community within the EU institutions.

2.3. Prior checks

2.3.1. The EDPS mandate

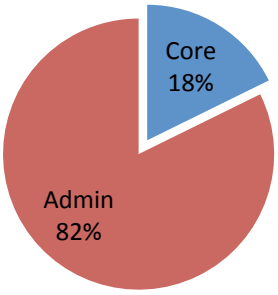
Regulation (EC) No 45/2001 provides that all processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes are to be subject to prior checking by the EDPS (Article 27(1)).

Article 27(2) of the Regulation contains a non-exhaustive list of processing operations that are likely to present specific risks. In case of doubt as to the need for prior checking, the DPO may consult the EDPS under Article 27(3). Prior checking is carried out by the EDPS following receipt of a notification from the DPO. Our final position on a processing operation is outlined in an Opinion, which is notified to those in charge of that operation and the DPO of the institution or body (Article 27(4)). The Opinion of the EDPS usually contains recommendations that the EDPS follows up.

A large number (80% in 2014) 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 inquiries. Our Guidelines (see point 2.7.1) on these common administrative procedures were designed to help EU institutions and bodies to comply with data protection principles and to share best practices. In cases where guidelines have been published, we issue short Opinions focusing only on aspects that diverge from them.

As we received a significant number of notifications in 2013 and 2014 and even larger number of recommendations to be followed-up, we developed a criteria to help us be more selective about

Notifications to the EDPS 2014
Core Business vs Administration



the recommendations we follow up. This selectivity allows us to concentrate our efforts on managing risky processing operations. Our other recommendations are followed up by the DPO of the relevant institution or body, in line with the principle of accountability.

The prior checking exercise provides a systematic way of learning about the activities of the EU institutions and bodies and allows the EDPS to understand patterns or shortcomings in the implementation of data protection principles. The prior checking activity is a matrix of knowledge for us; the high number of Opinions issued helps to build other supervisory tools such as inspections, surveys, inquiries, compliance and consultancy visits.

2.3.2. Prior checking in 2014

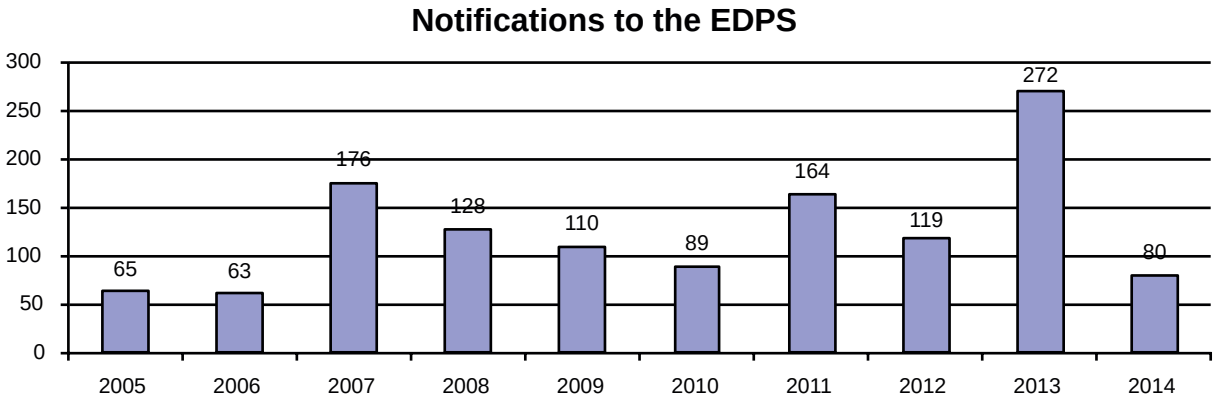
In 2014, we received 80 notifications for prior checking with one subsequently withdrawn. Progress continued to be made in clearing the back-log of *ex-post* notifications received in 2013.

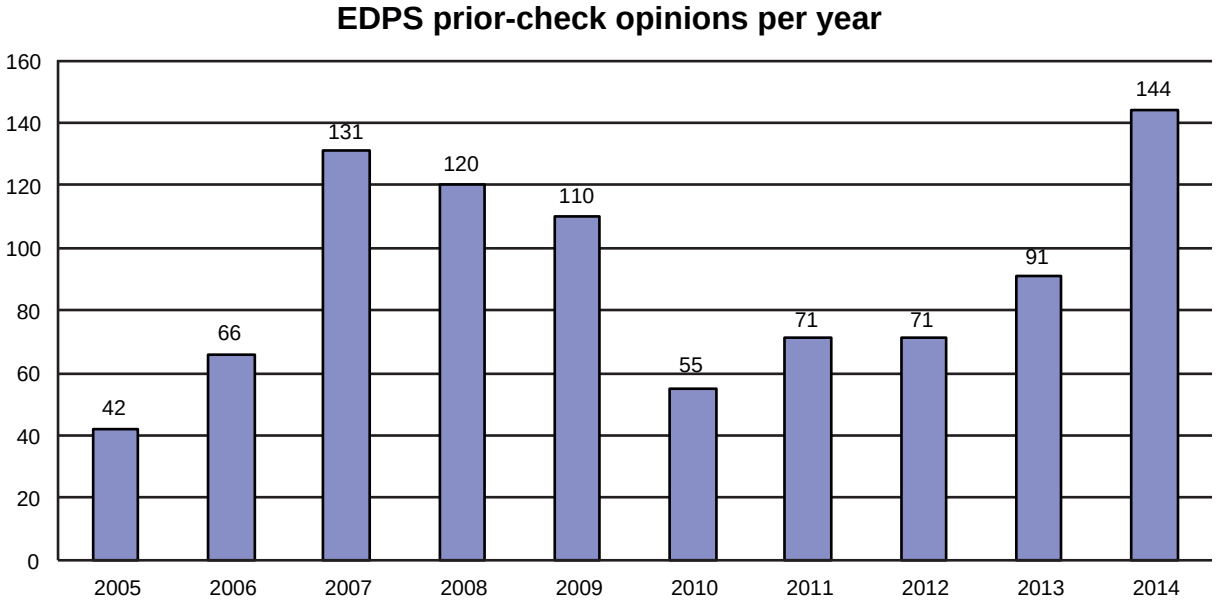
In 2014, we issued 144 prior check Opinions (an increase of approximately 58% from 2013) and 26 Opinions (a 24% increase from 2013) on 'non prior checks'[4]. In total, we examined 185 notifications, some of which led to joint Opinions. A variety of issues were analysed, some of which are reported below.

ARACHNE: no data protection cobweb

ARACHNE, a risk-analysis system, is part of the European Commission's fraud prevention and detection strategy in the area of Structural Funds (European Social Fund and European Regional Development

4 When a notification is received by the EDPS, but the processing operation does not fall within the scope of Article 27, the EDPS may nevertheless issue recommendations.





Fund). It complements an existing database with publicly available information in order to identify the most risky projects based on a set of risk indicators, which are used to help auditors in identifying and selecting future candidates for audit. Unlike other fraud detection processing operations, ARACHNE does not endeavour to assess the individual conduct of fund recipients or exclude beneficiaries from the funds.

The recommendations in our Opinion of 17 February 2014 refer, among other things, to the need to ensure data quality and the information to data subjects. Given that ARACHNE will, for example, contain information on individuals to whom sanctions are applied, we expressed a preference for the adoption of a more specific legal basis authorising the processing of special categories of personal data under Article 10(5) of the Regulation. During the follow-up phase, the European Commission has committed to future action on a variety of recommendations.

Bringing privacy in from the cold: asset freezing procedures at the Council

Asset freezing is one measure that can be taken against individuals suspected of certain serious crimes, such as terrorist activities, or human rights breaches committed by persons related to regimes in certain third countries. On the recommendation of member states, the European Council publishes lists of people whose assets should be frozen, together with the reasons, in the Official Journal of the European Union. Financial institutions are then obliged to block these accounts on the basis of these lists.

The EDPS was tasked with assessing the data protection implications of this process and, on 7 May 2014, we published our Opinion. In line with our approach from a previous Opinion, which addressed the asset freezing processing procedure used by the European Commission, we recommended that the Council limit the amount of information published in the lists. This would mean only

publishing what is really necessary to identify the individuals concerned. In particular, we expressed our doubts concerning whether it is truly necessary to publish the reasons why someone is listed.

Occasionally, a person is found to have been listed in error. This usually happens as a result of a mistake or because the grounds for listing no longer exist. This presents a problem as, although the Council 'de-lists' those who are wrongly cited, the fact that they were ever on the list remains on public record in the Official Journal. To address this, we recommended that the Council not only correct the lists without delay and at regular intervals, but that it also takes additional measures to clear the names of those who are wrongfully listed. This could be done, for instance, by providing the reasons for erasure in the amending act, which is published in the Official Journal, or in a letter to the person concerned. These steps should help those concerned to unblock their accounts and reduce any negative effect on their reputation. The EDPS is following up this case with the Council; several of the recommendations made have already been closed.

Dealing with allegations of scientific misconduct

To ensure the highest standards of research integrity, the European Research Council Executive Agency (ERC) has developed a procedure for dealing with any information it receives concerning alleged scientific misconduct. This term covers a wide range of possible cases, such as fraud and the violation of regulations.

In the context of proposals submitted to the ERC or projects financed by an ERC grant, the notion of scientific misconduct is interpreted in a broad sense and considered applicable whenever a person's behaviour jeopardises the value of science and, in particular, the reputation of those in the scientific community, as well as of the bodies funding or hosting these scientists. For example, if an author commits plagiarism or fails to comply with ethical standards when submitting a proposal to the ERC, that person is considered guilty of scientific misconduct.

As the agency receives allegations of scientific misconduct through various channels, including anonymously, we addressed the issues in our *Opinion* of 9 July 2014. We stressed the importance of taking the appropriate steps to ensure a high level of accuracy when dealing with personal data. We also welcomed that the person alleged to have acted in breach of good scientific conduct has the opportunity to comment on the allegations against them.

We noted that the ERC pays special attention to all individuals whose data might be collected as part of the procedure, such as that of informants. We reinforced that their identities should be kept confidential as long as this does not contravene national rules regarding judicial proceedings. As stated in the EDPS *Guidelines* on the Rights of Individuals with regard to the Processing of Personal Data[5], we reminded the ERC that data subjects have to be informed of the main reasons for any restriction to their right of access to their data and of their right to consult the EDPS in such cases.

Conducting an effective survey

We issued an Opinion on plans by the European Anti-Fraud Office (OLAF) to launch an analysis of the services it provides through human resources (HR). As part of its Human Resources Strategic Plan, the institution aims to develop an HR strategy which better serves employee needs.

The process involves each manager interviewing every jobholder individually. The answers from these interviews are recorded on a standard questionnaire composed of various entries, such as position in the unit, education, professional skills, previous training, comparison to ideal profile and training needs. The completed questionnaires are submitted to OLAF's HR unit for analysis, and managers are instructed not to retain any copies of the completed questionnaires, nor to use the data for performance evaluation purposes.

Our Opinion focused on the need to ensure the accuracy of the data collected. We recommended that this should be done by asking staff members to sign the questionnaire filled in by their manager

5 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf.

during the interview. Additionally, staff must clearly understand the purpose for which their data is being collected. Therefore, we also recommended that all participants should be informed that though the data gathered in the context of the '*needs analysis*' will not be used to assess performance, it will feed into the construction of individual training plans, the follow-up of which is part of the staff appraisal by their line manager.

2.4. Complaints

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).

2.4.1. The EDPS mandate

A complaint to the EDPS can only relate to the processing of personal information. The EDPS is not competent to deal with cases of general maladministration or, for instance, to modify the content of the documents that the complainant wants to challenge or to grant financial compensation for damages.

*The processing of personal information which is the subject of a complaint must be carried out by **one of the EU institutions or bodies**. Furthermore, the EDPS is not an appeal authority for the national data protection authorities.*

In principle, an individual can only complain to us about an alleged violation of his or her rights related to the protection of his or her personal information. However EU staff can complain about any alleged violation of data protection rules, whether the complainant is directly affected by the processing or not. The Staff Regulations of EU civil servants also allow for a complaint to the EDPS (Article 90b).

According to the Regulation, the EDPS can only investigate complaints submitted by **natural persons**. Complaints submitted by companies or other legal persons are in principle not admissible.

Complainants must also identify themselves. Anonymous requests are therefore not considered. However, anonymous information may be taken into account in the framework of another procedure (such as a self-initiated enquiry, or a request to send notification of a data processing operation, etc.).

It is to be noted that the **compliance rate with EDPS decisions is high.** The EDPS has, to date, never needed to apply coercive methods (e.g. referring a matter to the Court of Justice of the European Union) because of the good level of compliance with decisions. This does not exclude the possibility to use the powers described in Article 47 of the Regulation should the case justify such an action.

The EDPS shall decide on the most appropriate form and means to handle a complaint taking into account certain aspects (gravity of the alleged breach, time of the events, etc.). This means that the EDPS has a certain margin of manoeuvre in the admissibility of complaints.

Considering that, in general, the DPO is better placed to handle complaints; the complainant is advised to submit the complaint first to the DPO. If the complainant refuses to involve the DPO, the EDPS handles the case.

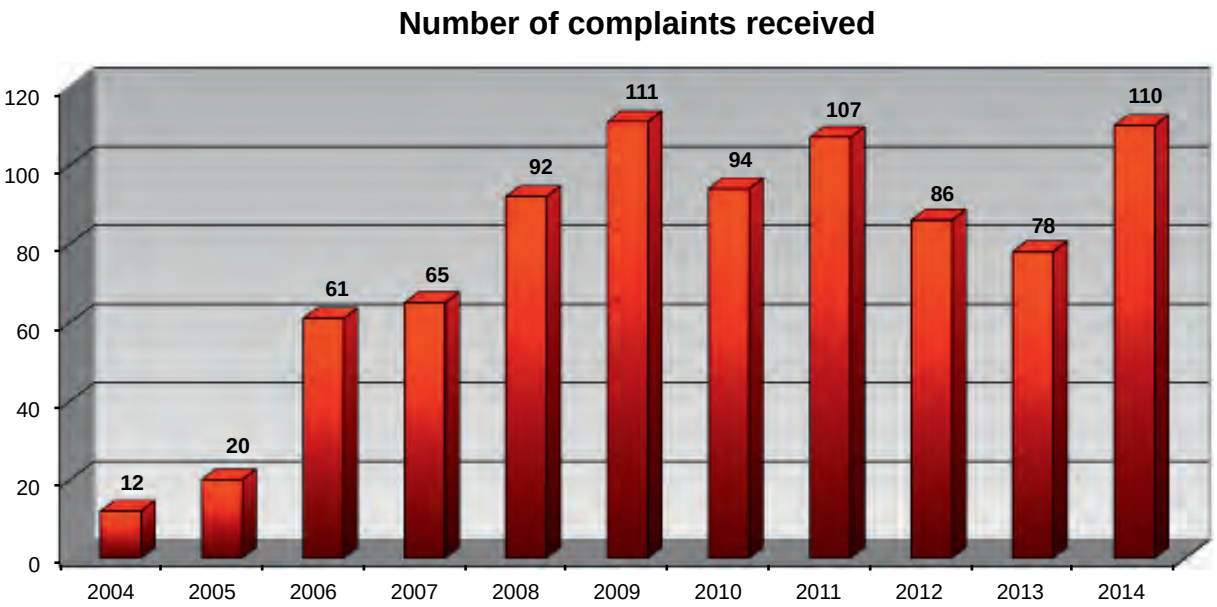
2.4.2. Complaints dealt with in 2014

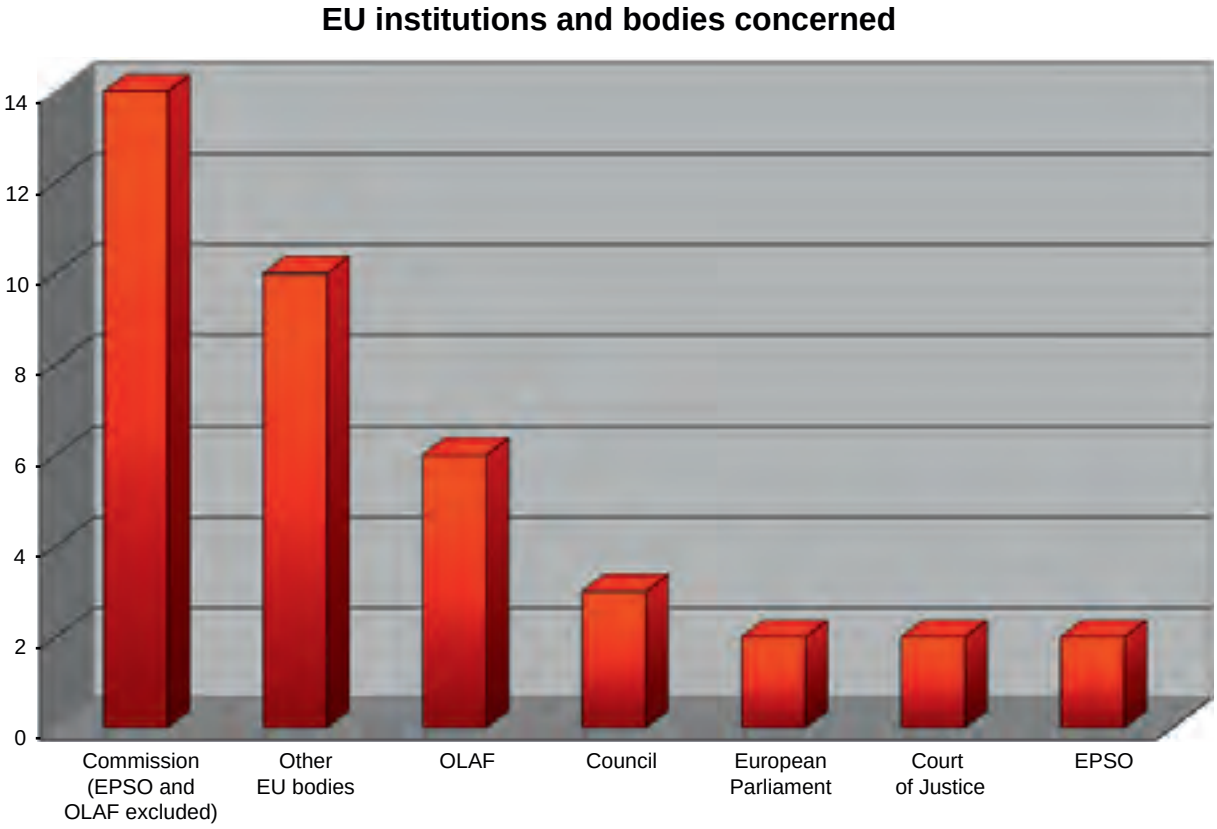
In 2014, the EDPS received 110 complaints, an increase of approximately 41% compared to 2013. Of these, 72 complaints were inadmissible, the majority relating to processing at national level as opposed to processing by an EU institution or body.

The remaining 39 complaints required in-depth inquiry, an increase of about 30% compared to 2013. In addition, 18 admissible complaints, submitted in previous years (three in 2011, three in 2012 and 12 in 2013), were still in the inquiry, review or follow-up phase on 31 December 2014.

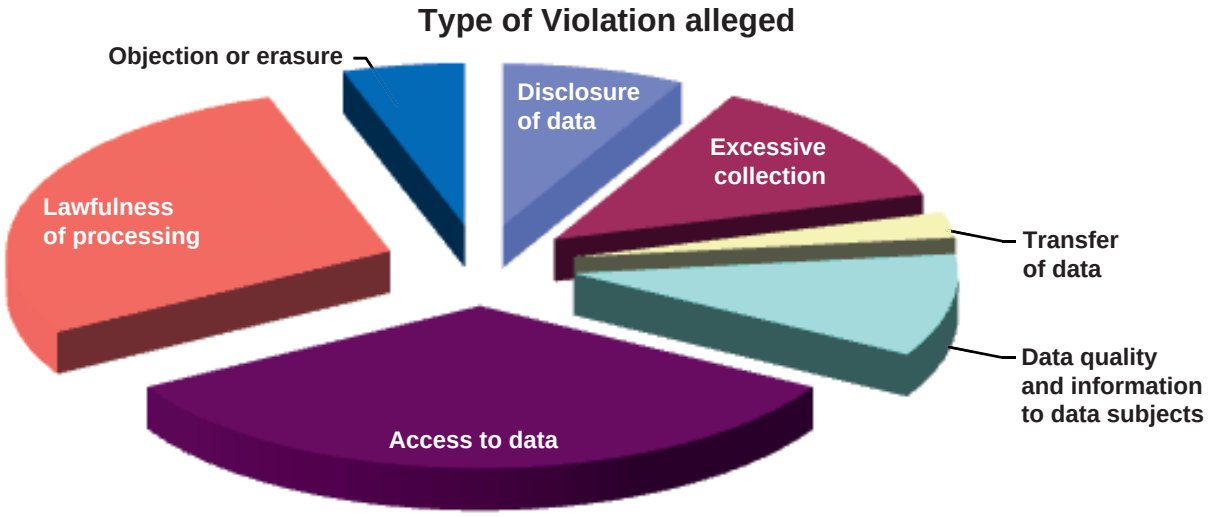
The EDPS receives a number of complaints with a **remote connection** to data protection. It may happen that complainants use the data protection channel because the case involves some kind of

processing activity, even if the problem is not a data protection issue (e.g. staff members disappointed with the result of the evaluation). In those cases, the EDPS has to clearly establish the limits of its competence and restrict the use of resources to the specific data protection implication of the case.





The following is a summary of a selection of complaint cases that we handled in 2014.



Your work emails, your personal data?

A former EU staff member submitted a complaint to the EDPS concerning access to his professional email account. This case required the analysis of what exactly should be considered personal data in this context.

Our assessment of this issue followed the approach taken in the Working Party 29 Paper[6] on the concept of personal data. On this basis, the email address, the name of the staff member when mentioned in emails and attachments, and the associated traffic information concerning when an email was sent or received by a staff member, are all considered to be the personal data of the person concerned. The content of emails and associated attachments within an email account, however, should only be considered the personal data of a staff member if they relate to him as a data subject. For example, this might include emails on evaluation, work contract related issues and internal investigations or procedures concerning the staff member, as well as the staff member's personal assessment of certain situations or conduct.

However, just because someone has a right of access to personal data does not mean that they are automatically entitled to receive copies of entire documents or emails. The action to be taken will depend on the circumstances: sometimes it will be necessary to provide a copy of the documents, but in other situations it might be more appropriate, for instance, to give direct access to them on the premises of the EU institution or body - which qualifies under the EU Regulation as 'communication in an intelligible form'.

Establishing a definition for personal data

In another case, the EDPS was required to adopt a Decision in a complaint case against the European Anti-Fraud Office (OLAF) which also required a preliminary analysis as to the scope of the concept of personal data. The complainant alleged, among other issues, that OLAF had not fully respected his right of access.

In dealing with the complainant, OLAF had applied a limited interpretation of Article 2(a) of Regulation 45/2001. The EDPS, however, considers that Article 2(a) of the Regulation specifies a much broader concept of personal data. Indeed, according to Article 2(a) of the Regulation, personal data is '*any information relating to an identified or identifiable natural person*'.

This definition clearly refers to more than just the name of an individual. Once again, we drew on the approach set out by the Article 29 Working Group[7] to support our decision. The Working Party 29 clarifies that information 'relating to' an individual, in the sense of Article 2(a), includes information concerning the identity, characteristics or behaviour of an individual; information used to determine or influence the way in which that person is treated or evaluated; and data that, if used, is likely to have an

6 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP 136).

7 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP 136).

impact on that individual's rights and interests. In light of this definition of personal data, the EDPS therefore requested that OLAF reconsider the answer it originally provided to the complainant's access request.

Addressing access to documents requests

The EDPS was asked to investigate an access to documents case involving the European Commission. The applicant was asked by the Commission to provide them with his postal address, a request which he found to be excessive.

After a full investigation of the case, we found several reasons why the collection of this personal information should be considered legitimate including:

- to ensure legal certainty as to when the reply was received;
- to counter requests for access under a false identity; and
- to verify whether the person requesting access to documents is situated in the European Economic Area.

Based on this, we decided that asking for an applicant's postal address was not an excessive requirement for access to documents requests. Nevertheless, it is important to provide applicants with information explaining why their postal details are needed. Accordingly, the Commission now includes this information in its privacy statement.

Your email account: for your eyes only?

The EDPS received a complaint from a former member of staff of an EU body, alleging that his email account (firstname.name@body.europa.eu) had not been deactivated after his departure. Instead, the account remained open and all of the emails he received were forwarded to the general functional mailbox of the EU body concerned, where they could be accessed by a large number of other staff members.

We found that the fact that the complainant's email account was not deactivated after his departure was a breach of the security rules of Regulation 45/2001. Furthermore, the subsequent automatic forwarding of the complainant's messages to the general functional mailbox was not only a breach

of the security rules but was also unlawful as it was not necessary.

Our Decision finds that the forwarding of e-mails from the account of a former employee should only be possible in exceptional circumstances, if it can be justified for reasons of business continuity. The EU body in question could have opted for less privacy intrusive measures when dealing with this case. Options to consider might have been:

(1) to set up an automatic response for the individual email account, asking for important correspondence to be resent to another email address; or

(2) to give one person, in cooperation with the DPO, authorisation to access the account.

Additionally, the EU body should have informed the complainant when it decided to forward his emails, thus allowing him to exercise his right to object.

We asked the EU body to act without delay. The EU body took the necessary steps to remedy the situation and therefore the case was closed.

Directory data breach

Due to a technical error, a European institution made information about its staff available on the internet which had only been collected for internal purposes. This information, meant for the internal network was publicly accessible on the internet for a certain period of time. Compared to the version that is supposed to be publicly available, this included job descriptions, first name and photo (where uploaded by the staff member in question). A staff member raised a complaint about this data breach. The EDPS investigated the case, including the organisation's breach response and came to the conclusion that a breach of Article 22 of the

data protection Regulation had indeed occurred. On the other hand, the EDPS was satisfied with the organisation's breach response and that it has taken the necessary measures to prevent similar breaches re-occurring.

Asset freezing

Several persons who had been subject to an asset freeze on the basis of Article 215 of the Treaty on the Functioning of the European Union complained about the processing of their personal data by the Council of the European Union. The complainants had successfully challenged their designation in Court and have since been delisted. However, the Council simply stated that they had been delisted and did not taken any further steps to publicly 'clear their names'. This 'public clearing' has been recommended by the EDPS in several prior check Opinions concerning asset freezing (see Section 2.3.2), among others because the initial publication of the names of the complainants as persons subject to an asset freeze in the Official Journal cannot be revoked. The EDPS found that the complainants are entitled to obtain deletion of their personal data processed by the Council under Article 16 of the data protection Regulation and that the Council should take additional measures to publicly clear the complainants' names.

2.5. 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 latest version of this **general stock taking exercise** is our 2013 Survey. In 2014, we carried out **targeted monitoring** exercises in cases where, as a result of our supervision activities, we had cause for concern about the level of compliance in specific institutions or bodies. These took the form of a one day **visit** to the body concerned with the aim of addressing the compliance failings. In addition, **inspections** were carried out in certain institutions and bodies to verify compliance on specific issues.*

2.5.1. Visits

A visit is a compliance tool, the aim of which is to engage the commitment of senior management of an institution or agency to comply with the Regulation. The visit comprises an on-site visit by the EDPS or Assistant EDPS and is followed-up with correspondence relating to a specific road map agreed between us and the institution or body visited. In promoting the notion of accountability, a visit is thus a way for us to take targeted action where necessary. We take the decision to visit usually when our monitoring shows that there has been a lack of compliance with the data protection rules, a lack of communication or simply to raise awareness.

The results of the visits can be measured in terms of raising awareness of data protection; raising the level of compliance via commitment of the management; increasing our knowledge of agencies and, in general, fostering better cooperation with the agencies visited.

We have recently developed a new type of on-site visit called **consultancy visits** where two members of EDPS staff are nominated as on-site consultants. This type of visit is a practical tool to tackle specific problems, raise awareness, improve cooperation and enhance the accountability of the targeted body. In one instance, we followed-up a consultancy visit with a short **secondment** of an EDPS member of staff.

Between January and December 2014, we visited four EU agencies: the European Investment Fund, the EU Satellite Centre, the GNSS Supervisory Authority and the EU Institute for Security Studies,

EIF

The European Investment Fund (EIF) is a public-private partnership with the EIB, the European Commission and several financial institutions as shareholders based in Luxembourg. Its core business is to provide risk finance to SMEs. The decision to visit the EIF was based on EIF's low scores in our 2013 compliance survey, which indicated no progress compared to our 2011 survey and because the respective roles of EIB and EIF in personal data processing lacked clarity. During the visit, we identified various areas of non-compliance, such as the clarity of the inventory and the lack of notifications under

both Articles 25 and 27 of the Regulation. The EIF committed to take measures in order to achieve compliance in the context of a mutually agreed roadmap and has in the meantime completed the inventory.

EU SatCen and GSA

The EU Satellite Centre (EU SatCen) and the GNSS Supervisory Authority (GSA) were also selected for a visit based on our 2013 Survey, where we had found communication to be a problem. Given that neither agency had provided sufficient evidence of satisfactory compliance by the deadline we set them, we decided to conduct these visits at working-level on issues ranging from human resources management to IT security and the tasks of different actors within the organisation. This involved trainings and Q&A sessions conducted by EDPS staff, with the aim of providing hands-on help to the agency and educating their staff and management on how best to integrate data protection principles into their working environment. Both agencies fully engaged with us and have expressed their commitment to improve compliance with data protection principles - both with a view to achieving full compliance for the 2015 general survey.

EUISS

The EU Institute for Security Studies (EUISS) was chosen for a visit because of its performance in the 2013 general survey. Although it used to be in a special situation as a former second pillar agency (common foreign and security policy), it has now become a 'regular' agency. This is also confirmed by the update of its legal basis adopted in early 2014. For practical reasons, the visit was split into a meeting between the EUISS Director and the Assistant Supervisor in June 2014 and a visit to the EUISS in Paris at staff level in October 2014. In the meeting between the Director and the Assistant Supervisor, EUISS stated a commitment to improve compliance. During the visit in Paris, EDPS staff met EUISS' newly appointed Head of Administration, the DPO and relevant staff for discussions and a training session on data protection principles. The test for improved compliance will be the 2015 general survey.

2.5.2. Inspections

Inspections are another tool for 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 or 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[8] contain the criteria the EDPS applies to launch an inspection; a 2013 Policy paper on inspections[9] further explains the EDPS' approach to inspections.

During the course of an inspection, we verify facts on-the-spot with the ultimate goal of ensuring compliance. Following an inspection, we always give appropriate feedback to the inspected institution.

In 2014, we continued the follow-up of previous inspections. In addition, we inspected Frontex, the European Parliament and conducted a targeted inspection on health data at the European Commission and the Council.

European Parliament

The collection and processing of the personal data of visitors, the accreditation of journalists as well as video-surveillance, concern a significant number of people and impact public perception of the European institutions and bodies, including the European Parliament (EP) for respecting fundamental rights in general. The inspection at the EP focussed on those three processing operations. Overall, we found a very satisfactory level of compliance with

8 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_guidelines_EN.pdf.

9 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_Policy_EN.pdf.

the commitments previously undertaken by the EP in the context of prior-checks and in the follow-up of complaints, such as data minimisation in pre-registering visitors.

Frontex

The inspection at the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU (Frontex) was part of our annual inspection plan for 2014 due to a delay in implementing the follow-up to our visit of December 2012 and because Frontex processes sensitive data as part of its core activities. It was an opportunity to acknowledge the progress made, and the follow-up of our recommendations on Frontex-specific applications delivered findings on issues related to the function of the data protection officer (DPO). In order to reap the benefits of a privacy-by-design approach and ensure compliance, planned processing operations need to be included in the DPO's inventory. The implementing rules on data processing issues including core business activities and relating to the DPO status should also be updated.

European Commission and Council

The targeted inspections at the Medical Service of the Commission and the Medical Service and the Welfare Unit of the Council focused on the obligation of professional secrecy for non-medical staff, such as secretaries and social workers; the handling and processing of personal information related to Commission and Council employees; and the physical and organisational security measures used to protect the health data processed by both institutions.

These inspections were particularly important due both to the size of the institutions, and thus the amount of data they process, and to the particularly sensitive and personal nature of the data involved. Subject to some improvement measures, we concluded that both institutions are in line with the relevant personal data protection rules, making this a good example of two large institutions applying the principle of accountability in the sensitive field of health data.

2.6. Consultations on administrative measures

2.6.1. The EDPS mandate

The EDPS issues Opinions on data protection matters, following a request either from an EU institution or on his own initiative. The EDPS may give an opinion on a decision or any other act of the administration of **general application** relating to the processing of personal data carried out by the EU institution concerned (Article 28(1)). The EDPS may also give advice on cases involving **specific processing activities or questions** on the interpretation of the Regulation (Article 46(d)).

The principle of **accountability** applies to the management of consultations. EU institutions should first seek the internal advice of their DPO and therefore involve their DPO when drawing up measures affecting the right to data protection. If the DPO is not in a position to provide an appropriate solution, the EDPS can be consulted. The consultation must relate to **new** or **complex issues** (no precedent in the field, lack of doctrine or lack of clarity in the definition of certain concepts of the Regulation).

Since 2014, the EDPS has dealt with **informal** consultations where the DPO is looking for advice but does not necessarily want to this to be known or if basic advice is sought; this takes place via an informal email exchange.

The consultation Opinions are published on the EDPS website. Communication of the Opinions plays a key role in the virtuous circle, helping DPOs and EU institutions to apply the accountability principle and distinguishing new or complex issues that deserve formal consultation to the EDPS.

2.6.2. Consultations in 2014

In 2014, we received 48 consultations on administrative measures. A variety of issues were examined, some of which are reported below.

Human error results in security breach

On 27 November 2013, the EDPS was made aware of an apparent breach of Regulation EC No 45/2001 involving the disclosure of candidates' email addresses following a recruitment application process at an EU agency. It transpired that an HR assistant sent out an email to inform 205 non-selected

candidates that they had not been successful in their applications for a specific post. In this particular case, a mistake was made by an assistant in the HR team who, instead of blind copying all the addresses in the 'BCC' field of the email, accidentally included them in the 'TO' field. We were satisfied that the agency had adequate preventative measures in place at the time of the incident, to minimise any risk to personal data. A number of further measures have been (or will be) implemented following the incident, to mitigate the risk of any other disclosures. We recognised that this particular data breach was caused by human error, which did not seem to have occurred as a result of an institutional negligence on the agency's part in terms of data security.

Data Protection principles V. Data retention

Whilst conducting an internal investigation at another European institution, investigators from the European Anti-Fraud Office (OLAF) requested the records of professional phone calls made from the professional mobile phone of the person under investigation. It transpired that several years' worth of data were available. However, under the EU Data Protection *Regulation*, the storage of such data for more than six months is not permitted, unless it is required for a court matter that is already pending at the end of this period. In the consultation, we were asked to consider whether these records could still be made available to OLAF. Given the fact that the retention of these documents was already unlawful, we advised that the records must not be provided to the investigators, but should be destroyed, along with any other communication records retained by the institution for more than six months. We also advised the institution concerned to put in place a system to ensure that retention periods are not exceeded in future. In response, both recommendations were implemented by the institution.

2.7. Data protection guidance

The experience gathered in the application of the Data Protection Regulation has enabled us to translate our expertise into generic guidance for institutions and bodies. In 2014, this took the form of guidance in the areas of data subject rights and transfers to third countries and international organisations, training for DPOs/DPCs, a dedicated area for DPOs on the EDPS website and a telephone helpline for DPOs.

2.7.1. Thematic Guidelines

In line with the action plan established in the EDPS Strategy 2013-2014 and the request from stakeholders for more guidance in the area of data protection, we have continued our work in the area of thematic guidelines. These cover not only areas subject to prior checking by the EDPS but also more horizontal themes.

- Data subject rights

In February 2014, we published guidelines on the Rights of Individuals with regard to the Processing of Personal Data.

The content of the guidelines is based on EDPS positions in the area of data subjects' rights, as developed in a series of EDPS Opinions on EU data processing operations. The guidelines describe our positions and recommendations on the relevant principles of Regulation 45/2001 and provide information on current best practice and other pertinent issues. For example, they highlight the broad concept of personal data under the Regulation, according to which personal data refers to much more than just the name of a particular individual.

While the EDPS guidelines have been developed for the EU institutions and bodies, they may offer valuable general guidance on fundamental rights for other public sector bodies. For instance, the guidelines highlight the delicate balance that the EDPS strikes between the rights of individuals whose personal information is processed and the rights and freedoms of others, such as whistleblowers or informants, who also need to be protected.

- ### Position paper on transfers

On 14 July 2014, we adopted a position paper designed to provide guidance to EU institutions and bodies on how to interpret and apply the rules laid down in Regulation (EC) No 45/2001, when transferring personal data internationally.

Our guidance focuses mainly on the methodological analysis that EU institutions and bodies have to conduct before transferring personal information to third countries or international organisations. Indeed, the principle of 'adequate protection' has to be respected in those cases. This principle requires that the fundamental right to data protection is guaranteed even when personal information is transferred outside the EU or to bodies not subject to EU law.

EU institutions and bodies should analyse the level of protection provided by the recipient of the data - adequacy should be determined by the nature of the data protection rules applicable at the destination, and the means for ensuring their effective application (supervision and enforcement).

In cases where the European Commission has adopted an 'Adequacy Decision' it is not necessary to further analyse the need for adequacy. Transfers are also allowed when the controller develops specific mechanisms that provide for appropriate safeguards. Finally, transfers without special safeguards are allowed in exceptional circumstances, provided that a specific derogation is applicable, such as the consent of the individual, important public interest, etc.

Examples are given to facilitate the task of data controllers and data protection officers (DPOs) in applying these rules, as well as a checklist with the steps to be followed when applying Article 9 of Regulation 45/2001. The paper also provides the relevant information on the supervisory and enforcement roles of the EDPS within the context of data transfers.

- ### Guidelines on the management of conflicts of interest

In December 2014, we published guidelines on the collection, processing and publication of personal data with regard to declarations relating to the management of conflicts of interest in EU institutions and bodies. The guidelines provide EU institutions and bodies with practical guidance on respecting the data protection rules and finding a balance between the public interest for transparency and the individual's rights to privacy and data protection. This balancing exercise can strengthen the efforts of institutions to foster the trust of the public as well as those who work for them. The guidelines cover declarations relating to the management of conflicts of interest by all persons working for EU institutions and bodies (i.e. persons employed by the EU and external experts) or appointed to high political and management posts, including, where applicable, their household members. Depending on the tasks of the individuals concerned, it can sometimes be necessary to publish those declarations to allow control by the public and peers. Such analysis must be made on a case-by-case basis, taking into account the tasks and responsibilities of the individual concerned.

2.7.2. Training and workshops

As part of the process of making EU institutions more accountable, we are keen on providing training and guidance for DPOs, DPCs and controllers so that they may better understand the data protection principles and their possible obligations.

On 28 January 2014, EU data protection day, we participated in a DPC meeting at the European Commission, delivering a speech on the Regulation (EC) 45/2001 in the light of the current reform of the general data protection framework. This was an occasion to reflect with the DPCs on the specificities of the Regulation as an instrument for EU public service and possible improvements that would be welcome in the revision of the instrument.

On 13 June 2014, we organised a general training for DPOs from EU institutions and bodies with a focus on the how to complete a notification form. We provided concrete examples on each principle evoked in the notification and the participants shared their experiences and doubts on several issues, such as data quality principle, access and rectification rights, transfers, security etc.

We also provided specific training sessions to staff of some agencies (FRONTEX) or their DPOs (ECDC, EUISS, EIF) on a request basis and one to trainees of the Council, Committee of the Regions and the Economic and Social Committee.

In June and December 2014, we gave presentations at training courses organised by the European Institute for Public Administration (EIPA) in Maastricht,

which was attended by DPOs, DPCs and controllers. We spoke about the specificities of Regulation (EC) 45/2001, the role of the EDPS in the context of our Supervision and Enforcement work and presented two case studies, one on international transfers of personal data and the other one on the right of access in the context of a complaint.

2.7.3. DPO Corner and other tools

The DPO corner of the EDPS website contains relevant information and practical tools to assist the DPOs in the performance of their tasks such as informative documents on the role and missions of the DPOs, a variety of templates and presentations to help DPOs in their awareness raising activities, summaries of recent developments in the data protection arena, and an events list (training courses or meetings). This information is updated on a regular basis.

We also have a 'helpline' to reply to basic questions from DPOs or redirect them to a case officer who can answer their queries on a particular theme or case (see Section 2.2 on Data Protection Officers).

3. CONSULTATION

Our strategic objective

Ensure that the EU legislator (Commission, Parliament and Council) is aware of data protection requirements and integrates data protection in new legislation.

3.1. Our active policy role

Our policy work aims to advance the fundamental rights to privacy and data protection as its importance increases in the midst of rapid globalisation and technological development. We advise EU institutions and bodies on preparing legislation and policies which uphold these rights. This consultative role relates to proposals for new legislation and international agreements as well as soft law instruments like Commission communications or the positions of the EU and its institutions and bodies in international fora. We assess the legal aspects of new technology developments that may have an impact on data protection.

As described in our policy paper, the strategic objective underlying the interventions by the EDPS is to ensure that both the European Commission, as most frequent initiator, and the European Parliament and the Council as co-legislators, are aware of data protection requirements and integrate data protection in new legislation. We engage constructively with the European Parliament, the Council and the Commission and remain available to provide targeted and timely advice at any stage of the EU decision-making process. We act selectively on the basis of the priorities set out in our strategy, the annual management plan, and our inventory. Consequently, we focus our attention and efforts on areas that present the highest risk of non-compliance or where the impact on privacy and data protection are greatest.

3.2. Policy trends and priorities

Our aim is for high standards of data protection to be integrated in all new legislation.[10]

10 EDPS Strategy 2013-2014, 'Towards excellence in data protection', 22 January 2013.

Under Article 28(2) of Regulation 45/2001, the Commission has an obligation to consult the EDPS whenever it adopts a legislative proposal which relates to the protection of individuals' rights and freedoms in the processing of personal data. Under Article 41 of the Regulation, the EDPS is responsible for ensuring fundamental rights and freedoms of individuals are respected and for advising all EU institutions and bodies on processing of personal information.

3.2.1. Formal and public advice to the institutions

Where an initiative raises significant questions of compliance with data protection rules and principles, be it a formal Commission proposal for a legal act or a communication setting out policy orientations, we issue Opinions which analyse these implications in depth. In 2014, we published 14 such Opinions.

We issued more limited advice, or formal comments, on 13 policy initiatives, in most cases within two months after the adoption by the Commission of the document in question.

In 2014, we provided advice in several sectors such as transport policy, taxation and customs for the first time.

We also issued a 'preliminary Opinion', on the interplay between competition, consumer and data protection law in the digital economy. The Opinion addressed the general topic from the perspective of the increasing importance of data protection.

3.2.2. Informal advice

The scope of our advisory role is broad and we remain available to provide advice to the EU institutions at all stages. In line with established practice, the EDPS is consulted by the Commission informally before it adopts a proposal with data protection implications. In 2014, we provided informal comments on 33 separate draft initiatives. In addition, we had informal discussions with rapporteurs and shadow rapporteurs in the European Parliament and with the Presidency of the Council. Other means of providing advice included

presentations, explanatory letters, and hosting events with experts.

3.2.3. More proactive policy advice

In 2014, we reviewed how we fulfil this legal obligation to advise the institutions. In our June policy paper, '*The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience*'[11], we reiterated our principles of impartiality, integrity, transparency and pragmatism and our broad, inclusive and proactive engagement with stakeholders. We aim to develop a culture of accountability across all EU institutions and bodies through training and general as well as sector specific guidance to enable the institutions to make informed decisions on the data protection impacts of new proposals.

We have already begun to target engagement with less familiar interlocutors including the Commission's internal market and services directorate general (DG MARKT) and the Council presidency who are increasingly aware of the relevance of data protection. In addition, we have established regular liaison and information sharing with the Fundamental Rights Agency (FRA) and international bodies including the Council of Europe.

11 EDPS Policy Paper, 'The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience', 4 June 2014.

On the basis of constructive and targeted dialogue with the institutions, we specifically undertook to develop a 'policy toolkit' – including thematic or sectoral guidelines – for guiding policy and law makers on the relevance of the fundamental rights to privacy and to data protection in specific sectors.

In November 2014, we delivered the first of these tools focusing on financial services regulation, an area of intense legislative reform in recent years. Our sector guidelines built on insights gained during a seminar hosted by DG MARKT in February 2014.

3.3. 2014 Priorities

With regard to specific initiatives, our 2014 'inventory' anticipated five key areas of strategic importance for data protection. Our work under these headings is summarised below.

- Towards a new legal framework for data protection
- Rebuilding trust in global data flows in the aftermath of PRISM
- Initiatives to boost economic growth and the Digital Agenda
- Further developing the area of freedom, security and justice
- Reform of the financial sector.

3.3.1. Towards a new legal framework for data protection: An end in sight?

Reforming the data protection framework has constituted one of the largest and most complex challenges for EU lawmakers in recent years. There is great interest at national, European and international level in the evolution of the two draft proposals - for a General Data Protection Regulation, and for a Directive on personal data processed for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The EDPS continued to work closely with the Parliament, the Council and the Commission during the critical negotiations which took place in 2014.

In February, we wrote to the President of the Council of the EU addressing three crucial aspects of the reform under discussion.

- First, we explained the importance of keeping the public sector within the scope of the proposed General Data Protection Regulation, not least because of the growing trend for services which rely heavily on personal data processing, health care for example, to be provided by either private or public sector. It is perfectly possible to ensure that the new GDPR does not have the effect of lowering existing data protection standards applicable to public authorities.

- Second, we addressed the hotly debated 'one stop shop' principle whereby one single supervisory authority would be responsible for monitoring and taking decisions on the processing operations of a data controller or processor active in more than one member state, crucial, in our Opinion for harmonising the data protection framework while preserving the rights of individuals to an effective judicial remedy and to a fair trial.

- Third, we advised on the principle of accountability and the 'risk-based approach' for directing compliance efforts towards areas where they are needed most. We argued that controllers must apply clear criteria for assessing risk in order to avoid arbitrary and opaque decisions on processing operations, including those involving so-called 'pseudonymised data'.

On 5 November 2014, together with the Representative to the EU of the State of North Rhine-Westphalia, we co-hosted an event to examine the state of the negotiations on the reform package. Over 200 experts including the MEP rapporteur, representatives of the Council Presidency and the European Commission and the Chair of the Article 29 Working Party, discussed how data protection cuts across EU and national competences and has huge significance for both the single market and fundamental rights in the context of rapid technological development. The EDPS called for a sense of urgency in updating EU rules for the digital era.

3.3.2. Rebuilding trust in global data flows in the aftermath of PRISM

The mass surveillance of EU citizens by intelligence agencies and law enforcement agencies which was revealed in 2013 clearly flouted individuals' rights to privacy and to the protection of personal data. The EDPS addressed the public hearing of the European Parliament's Civil Liberties Committee in October 2013, emphasising serious concerns and the need for the EU to assert control of our privacy. We developed this message in our Opinion of 20 February 2014 on the Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows'. Correct enforcement of existing European data protection laws and international norms such as the European Convention of Human Rights (ECHR) were central to stop breaches to fundamental rights and freedoms, and repairing trust between Europe and the US. We expressed support for a privacy act in the United States, and called for the promotion of international privacy standards alongside the swift adoption of reforms to the EU data protection framework.

3.3.3. Initiatives to bolster economic growth and the Digital Agenda

The EDPS has engaged constructively on a broad range of policy developments as varied as competitiveness and consumer protection, internet governance, the functioning of the internal market, the single digital market, and customs and agriculture. We have also closely monitored the developments concerning the Safe Harbour agreement, and the Commission negotiations of new trade agreements (e.g. TTIP, TISA) as regards their potential impact on privacy and data protection.

3.3.3.1. Competition, consumer protection, privacy and Big Data

The collection and control of massive amounts of personal information are a source of market power for the biggest players in the online marketplace. Many consumers are unaware that their personal information is the currency they use to purchase services over the internet which are marketed as 'free', and that it is an increasingly valuable intangible asset for companies doing business in the EU. In our March 2014 Preliminary Opinion on privacy and competitiveness in the age of big data, we argued that these markets were exposing a complex interplay between EU law on data protection, competition and consumers, which now requires closer interaction between regulators in the different fields. Smarter interactions across these apparently silo policy areas will support growth and innovation and minimise the potential harm to consumers. We have continued to facilitate discussions between regulators and experts in these fields on this topic of growing concern. In April, the EDPS addressed the Consumer Forum and in June we hosted a workshop also involving the European Commission, the OECD and the US Federal Trade Commission.

3.3.3.2. Rules governing the internet

A sustainable model of internet governance is a necessary complement to data protection reform. In our Opinion of June 2014 on the Commission communication on '*Internet Policy and Governance – Europe's role in shaping the future of Internet Governance*', we urged the European Commission to take a leading role in facilitating the adoption of common data protection rules and standards across jurisdictions, consistent with the global reach of the internet.

The Internet Corporation for Assigned Names and Numbers (ICANN) initiated a public consultation on data collection and retention within the context of its 2013 Registrar Contract, which aims to encourage accountability and transparency in the domain name industry. In a letter to ICANN's General Counsel and Secretary on 17 April 2014, the EDPS encouraged the body to take the lead to ensure that when new tools, instruments or internet policies are designed, privacy and data protection are embedded in them by default (privacy by design) for the benefit of all – not only European - internet users. We advised the registrar contract should require 'by default' only the collection of those personal data which are genuinely necessary for the fulfilment of the contract between the registrar and the registrant - such as for billing - or for other compatible purposes such as fighting fraud related to domain name registration. In addition, this data should not be retained for longer than is necessary for these purposes, nor for any other purposes, such as law enforcement or the enforcement of copyright.

3.3.3.3. Regulating the internal market for civil-use drones

Remotely piloted aircraft systems (RPAS, commonly known as drones) operate without an on-board pilot. Their use for military purposes is fairly well known, but they also have a broad range of potential civil uses, including monitoring infrastructure, journalism, agriculture, law enforcement, public order and disaster response, logistics and various private activities like photography. Drones combine simple aircraft systems with devices such as cameras, microphones, sensors and GPS technology

which gather and process personal information – through, for example, facial recognition - to a degree which could seriously interfere with individual's rights to privacy and data protection. The Commission announced its support for the development in the market for drones in its Communication, '*A new era for aviation – Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*', advocating harmonisation of member state aviation safety policy and other compliance issues. The EDPS issued an Opinion in November 2014 emphasising that drones were only likely to be accepted by society if they integrated high standards of data protection and privacy enhancements at the design stage and were operated in full compliance with application data protection rules and principles. Although the EU's competence on regulation is limited to larger aircraft, EU data protection requirements apply irrespective of the size of the drones. We recommended that the EU take the lead in raising awareness of data protection rules, support implementation of privacy by design, require any EU regulation of the sales of drones to include privacy notices for small aircraft and require users of drones to assess the privacy impact of their actions.

3.3.3.4. Commercial use of data collected by earth observation satellites

Earth observation satellites generate high resolution data (HRSD) valuable for environment monitoring, urban planning, agriculture, natural resources management and disaster and emergency management, security and defence. Satellite operators distribute these data to commercial concerns such as geo-information service providers which can in turn be sold on to businesses and combined with other datasets including personal information. In 2014, the Commission proposed a directive setting out rules for the dissemination of HRSD. In our formal comments of July 2014, we noted that while HRSD technology did not so far allow for the direct identification of individuals, this could change in the future. Given the strong possibility and the routine combination of HRSD with personal information available to value added services, we recommended the inclusion of a provision for processing to comply with EU and national data protection rules.

3.3.3.5. Trade secrets

As part of the strategy for a Single Market for Intellectual Property Rights, the Commission adopted a proposal for a Directive on the protection of trade secrets from unlawful acquisition, use and disclosure in late 2013. Trade secrets are, according to the proposal, business information which 'extends beyond technological knowledge to commercial data such as information on customers and suppliers', and this includes personal data. The proposed directive focuses on the rights of the person or company who holds the trade secret to sufficient and comparable level of redress across the internal market where the information is unlawfully obtained or used. As we pointed out in our Opinion of March 2014, the trade secret holder also has obligations towards the individuals whose personal information is being processed. We recommended clarification of the relationship between personal data and the concept of trade secrets, and including provisions to ensure the protection of trade secrets in no way infringes upon the data protection rights of EU citizens, particularly their right to access the data being processed.

3.3.3.6. EURES job mobility portal

The 'EURES' database provides information, guidance and recruitment services to job-seekers throughout the EU. It allows you to upload CVs and search and apply for jobs, while employers can search the database for CVs which match their job vacancies. EURES is being upgraded and the Commission proposed a new regulation updating the portal's legal framework. In our Opinion of April 2014 on the proposal, we welcomed the inclusion of a requirement for explicit consent from job-seekers to the processing of their personal information via the portal, and of safeguards for their rights to access and to correct their

data. We recommended specifying more clearly who could access the database and ensuring that persons searching the database would only be able to access CV and contact data where the job-seeker had explicitly chosen to make their entire CV available for review by potential employers. In all other cases, potential employers consulting the database will only be notified of the fact that there is a match for their search specifications. We also recommended clearer specifications and limitations on the purpose of processing; clarifications on how automated matching would work; and the inclusion of safeguards against misuse of the system.

3.3.3.7. Single member private limited liability companies

The proposal for a directive on single member private limited liability companies is designed to make it easier for any potential company founder, and in particular for SMEs, to set-up companies in other EU member states. It aims to do this through harmonising 'the conditions of setting-up and operation of single-member limited liability companies'. In order to ensure transparency, the proposal requires registration and/or publication of certain information about the single-member company, some of which might include personal information. In our Opinion of July 2014, we welcomed the safeguards the Commission had included in their proposal, such as limiting the collection of data on an individual's disqualification to those which are currently in effect, so excluding the processing of historic data. We recommended further improvements, including more explicit text on what personal data, such as on disqualifications, may be exchanged via the internal-market information system (IMI), applying the proportionality principle and safeguards in decisions to disclose the identity of the single member in a public register (or in a register kept by the company and accessible to the public) where that single-member is an individual.

3.3.3.8. Information sharing for the prevention and deterrence of undeclared work

The Commission proposed a 'European Platform' to facilitate information exchange between national enforcement authorities, the Commission and other relevant organisations in the prevention and deterrence of undeclared work. The platform would look into how to improve data sharing including through use of the Internal Market Information System and the Electronic Exchange of Social Security Information. The focus would initially be on policies and measures put in place by the member states to tackle undeclared work, rather than the personal data relating to any individual undeclared workers or individuals or organisations that employ workers without declaring them. In our comments in July 2014, we welcomed this clarification and undertook to provide advice on any future plans to facilitate personal data exchange through the Platform.

3.3.3.9. Cross-border social security fraud

Member states exchange personal information in combating cross-border social security fraud. One suggestion for improving effectiveness of these procedures is more systematic 'data matching' in order to identify inconsistencies between sets of data held by different member states relating to the same individual. For example, a list of deaths which have occurred in a member state could be checked by other member states against records of pension and social security payment to prevent fraudulent claims on behalf of deceased residents in another member state. At the request of the Commission, we provided preliminary comments in January 2014 on a possible proposal for amending Regulation (EC) No 883/2004 on the coordination of social security systems. We recommended ensuring clarity on the nature, necessity and proportionality of any data-matching practice, ensuring that it would not result automatically in any denial of benefits and guaranteeing fair procedures for individuals to contest any decisions that were taken on the basis of automatic matching procedures.

3.3.3.10. EU-China Customs agreement

Mutual recognition between the customs authorities of the EU and China is intended to facilitate the operations of businesses which have invested in compliance and supply chain security and have been certified under their respective trade partnership programmes.

Data protection safeguards are essential in international customs agreements. In our Opinion of 14 March 2014, we welcomed the Commission's efforts to address this need, but recommended more be done to comply with the requirement that data protection standards be adequate for

international transfers of data. In February 2014, the Commission published its proposal for a Council Decision on the position to be adopted, on behalf of the EU, in the EU-China Joint Customs Cooperation Committee on mutual recognition of the Authorised Economic Operator Programme in the EU and Measures on Classified Management of Enterprises Program in the People's Republic of China.

We queried the practical enforceability of data protection safeguards, particularly given the absence of an independent data protection supervisory authority in the People's Republic of China. We made multiple recommendations including confirmation that the draft decision is binding on both parties and will prevail over Chinese national laws. We asked for greater clarity, for example on categories of data to be exchanged, who would be responsible for the data processing in the EU, ensuring that data subjects are able to exercise their rights, with procedures for ensuring redress for possible damages resulting from the acts and omissions of the Chinese authorities.

3.3.3.11. Customs and agriculture mutual assistance

Combating breaches involves extensive exchanges of information - including personal data – between competent authorities in the member states and the Commission. The aim of the Commission's proposal, for amending Regulation (EC) No 515/97 on mutual assistance and cooperation between the administrative authorities of the member states and the Commission to ensure the correct application of the law on customs and agricultural matters, was to improve this cooperation. New obligations were proposed for carriers to supply the Commission with information on container movements and amending rules on the central database for import, export and transit data to allow better analysis of the flow of goods. The Commission would be able to obtain supporting documents for import and export declarations directly from private sector operators.

In our Opinion of 11 March 2014, we argued for a single instrument based exclusively on the Treaty on the Functioning of the EU (TFEU), in order to guarantee legal certainty, a seamless data protection regime and coordinated supervision by national authorities and the EDPS of the several databases which involve the processing of personal data, including the Customs Information System. We recommended clarification on which rules apply when competent authorities handle personal data and more uniform provisions for data security.

3.3.4. Further developing the Area of Freedom, Security and Justice

In 2014, as well as considering a number of specific initiatives, such as the future of Europol, Eurojust and the creation of a public prosecutor's office, gun control and asset freezing, the EU took stock of its progress towards the creation of an area of freedom, security and justice. We continued to be active in shaping this broad agenda.

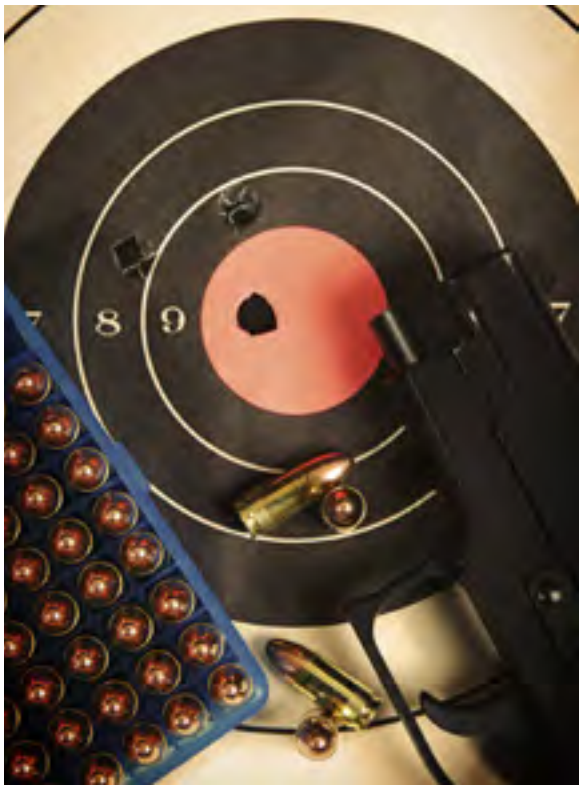
3.3.4.1. Post Stockholm JHA guidelines

The EDPS has called upon the European Council to place the rights of individuals at the core of justice and security policies in the years to come. The Parliament, the Council and the Commission provided input towards strategic guidelines under the current treaties for further legislative and operational planning in the area of freedom, security and justice. In our Opinion of June 2014, we argued that this was an opportunity to revitalise the EU's approach in these areas and to repair the loss of trust resulting from the revelations about mass surveillance. We highlighted the need for fuller integration of privacy and data protection in the activities of all EU institutions, citing as a wake-up call, the European Court of Justice's recent annulment of the data retention directive as an excessive violation of individuals' rights to personal data protection. We offered to work with the institutions to develop sector specific guidelines in this area on how to ensure proper limitations and safeguards in a more informed and systematic manner when launching proposals which have a significant impact on fundamental rights. We followed up this Opinion with a letter to the President of the European Council urging member states to commit to the adoption of reform data protection framework.

3.3.4.2. Strategy for the control of firearms

In 2013, the Commission proposed a wide ranging strategy on firearms, pointing towards future rules on the marking or implanting of biometric sensors in weapons, requirement of medical and criminal checks as a condition for the lawful purchase and ownership of any firearm and greater information between law enforcement and customs authorities,

particularly through large-scale IT systems. In our Opinion of February 2014, we highlighted the relevance of data protection rules for such measures and recommended that they be addressed through consultation at an early stage of the legislative process.



3.3.4.3. Asset freezing

Asset freezing is one measure that can be taken against individuals suspected of certain serious crimes, such as terrorist activities, or human rights breaches committed by persons related to regimes in certain third countries. On the recommendation of member states, the European Council publishes lists of people whose assets should be frozen, together with the reasons, in the Official Journal of the European Union. Financial institutions are then obliged to block these accounts on the basis of these lists.

The EDPS was tasked with assessing the data protection implications of this process and, in May 2014 we published our Opinion. In line with our approach from a previous Opinion, which addressed the asset freezing processing procedure used by the European Commission, we recommended that the Council limit the amount of information published in the lists. This would mean only publishing what is really necessary to identify the individuals concerned. In particular, we expressed our doubts concerning whether it is truly necessary to publish the reasons why someone is listed.

Occasionally, a person is found to have been listed in error. This usually happens as a result of a mistake or because the grounds for listing no longer exist. This presents a problem as, although the Council 'de-lists' those who are wrongly cited, the fact that they were ever on the list remains on public record in the Official Journal. To address this, we recommended that the Council not only correct the lists without delay and at regular intervals, but that it also takes additional measures to clear the names of those who are wrongfully listed. This could be done, for instance, by providing the reasons for erasure in the amending act, which is published in the Official Journal, or in a letter to the person concerned. These steps should help those concerned to unblock their accounts and reduce any negative effects on their reputation.

3.3.4.4. Reforming judicial cooperation and protection of the EU's financial interests

The Commission proposed reforming Eurojust, the agency for coordination of judicial investigation and prosecutions alongside the creation of a European Public Prosecutor's Office in the interests of a more coherent European system for the investigation and prosecution of offences affecting the Union's financial interests. These activities rely on processing of personal data. In our Opinion of March 2014, we welcomed the reference to applicable data protection rules, in particular those set forth in Regulation No 45/2001. We argued that, on the basis that the activities by these bodies could not be assimilated to genuine judicial activities, and that the processing of personal data by these bodies should be subject to independent supervision, the EDPS was the appropriate body to fulfil this role in closer cooperation with national data protection authorities. We made a number of specific recommendations to improve the text on issues such as

access to the case management system, data retention periods, the exercise of data subjects' right of access, and international data transfers.

3.3.4.5. European e-Justice Portal

Since its launch in 2010, the e-Justice Portal, intended to allow interconnection of national registers on criminal records, insolvency registers, business registers, land registers and so on, has been managed by the Commission in close cooperation with the member states. The portal aims to help establish the European judicial area by facilitating and enhancing access to justice and leveraging information and communication technologies to facilitate cross-border electronic judicial proceedings and judicial cooperation. In June 2014, the Commission adopted a decision on data protection in the portal given its readiness for the first interconnection of national registers involving the processing of personal data. The Commission Decision was a further step towards the adoption of a draft Regulation on e-justice. In our Opinion of September 2014, we encouraged the Commission in the interests of legal certainty, to ensure this draft regulation clearly sets out the terms on which specific national databases would be interconnected, the legal grounds for personal data processing and the responsibilities of controllers and processors in particular with regard to data security and data protection by design, purpose limitation and appropriate restrictions on any data combination.

3.3.4.6. Terrorist finance tracking

The EU-US Terrorist Finance Tracking Program (TFTP) is used to gather intelligence and prevent terrorist attacks through the sharing of information about financial transactions between the EU and the USA. Article 11 of the EU-US TFTP commits the European Commission to carrying out a study on the possible introduction of an EU system equivalent to the TFTP, the TFTS (Terrorist Finance Tracking System), which would allow for a more targeted transfer of data from the EU to the USA. Under this system, the EU would have more control over its citizens' data than the current agreement, which is considered by many to put EU citizens' data at risk. The impact assessment conducted by the Commission regarding the creation of the TFTS - a legal and technical framework for the extraction of data on EU territory - contains an analysis based on the principles of necessity, proportionality, cost-effectiveness and the safeguarding of fundamental rights. Taking all of this into account, the Commission has concluded that '*the case to present at this stage a proposal for an EU TFTS is not clearly demonstrated*'.

In our formal comments of April 2014, we welcomed this conclusion and the reasoning behind it. We regretted the Commission's choice not to apply the same analysis to the question of whether to continue, amend or terminate the existing EU-US TFTP agreement, particularly in the wake of the 2013 surveillance revelations and the judgement from the Court of Justice of the European Union (Joined Cases C-293/12 and C-594/12 Digital Rights Ireland), which found Directive 2006/24/EC to be invalid. We argued that a thorough investigation of the other options available to the EU in place of a TFTS was overdue, given the many questions as to the reliability and security of the TFTP agreement contained in various reports, including those of the Joint Supervisory Body of Europol on its inspections regarding implementation of the Agreement, the Article 29 Working Party analysis on the massive nature of transfers of financial data from the EU to the US and the limits of effective judicial and administrative redress.

3.3.5. Reform of the financial sector

The EDPS has been developing its expertise in how to apply data protection standards in the design and implementation of financial services regulation. We have issued our first set of guidelines for the sector, and provided advice on specific proposed measures in the areas of shareholder rights, resilience of the banking system and transparency in securities financial transactions.

3.3.5.1. Financial guidelines

Since the onset of the financial crisis in 2008, over 40 new laws on financial services regulation, many of which involve the collection, use and storage of large amounts of personal information by industry

and by regulators have been introduced. The EDPS has put together in a single, practical document our advice for embedding data protection rules and principles in current and future regulatory initiatives in this important sector. We explain how policymakers can balance the objectives of accountability and transparency with respect for the rights and interests of individual clients and employees. In a step-by-step guide, the document describes how to observe data protection rules in devising schemes for publication of sanctions in case of breaches of financial services rules, for corporate whistleblowing and for monitoring communications for the purposes of preventing and combating abuse and malpractice. We will continue to work closely with the institutions and will review the guidelines in light of feedback from policymakers about their usefulness.

3.3.5.2. Shareholders Rights Directive

As part of a proposal for greater transparency and encouraging long-term shareholder engagement, companies would have the 'right' to identify their shareholders and would be required to publicly disclose the remuneration of individual directors as part of the 'remuneration report' that shareholders would have the right to vote on. In our Opinion of April 2014 on the Commission proposal for amending Directives 2007/36/EC and Directive 2013/34/EU, we said that such measures require appropriate limitations and safeguards for individual's rights to privacy and data protection. We recommended clarity in the text on the purposes of personal data processing and prohibition on the use of information regarding the identity of the shareholders and remuneration of individual directors for incompatible purposes. We also recommended that companies be required to put in place technical and organisational measures to limit accessibility of the information regarding individuals such as shareholders or individual directors after a certain period of time. Finally, we recommended that where the disclosure of the details of an individual director's remuneration package revealed health data or other 'more sensitive' data, the information should be redacted so as to exclude any reference to such information.

3.3.5.3. Resilience of the European banking system and Reporting and transparency securities financing transactions

On 11 July 2014, we published an Opinion on two Commission proposals. The first of these concerned the resilience of the European banking system. The second addressed reporting and transparency securities financing transactions or, more simply, lending and borrowing activities associated with shadow banking.

As with previous proposals in the area of financial services regulation, we recommended implementing appropriate safeguards against the mishandling of personal information. For instance, we advised that, when an individual breaches the rules, the publication of warnings and sanctions about this identified individual should not be automatic. Instead, each individual should be assessed on a case-by-case basis, taking into account the need and proportionality of publishing their personal details.

3.4. Other policy initiatives

3.4.1. Application of food and feed law

A new Regulation on official controls and other official activities performed to ensure the application of food and feed law is still being discussed by the European Parliament and Council. The proposal envisages the processing of two general sets of data, namely data related to operators, such as individual or company's names, place of establishment, websites, ratings etc. and data related to the operators' assets, such as animals and goods. It also outlines the exchange of information between national competent authorities via an EU wide IT network, the IMSOC. In our comments of 20 February 2014, we clarified that:

- data concerning goods and animals could relate to an identified or identifiable individual operator, thus falling within the concept of personal data;

- data protection rules apply to the processing of data envisaged by the Regulation in so far as data relates to an operator who runs their business as a natural person, or the official title of the legal person identifies one or more natural persons, or other information about legal persons may be also considered as 'relating to' natural persons, or if the national laws, including those implementing Directive No 95/46/EC at domestic level, extend the protection of personal data to legal persons as well;

- IMSOC shall implement the concept of privacy by design and by default and the Commission shall bear the responsibility of its controllership for the exchange of personal data within the system, including providing data subjects with a first 'layer' of data protection notice and other relevant information on its multilingual website, also 'on behalf of' competent authorities.

3.4.2. EU-wide real-time traffic information services

Between December 2013 and March 2014, the European Commission conducted a public consultation on EU-wide real-time traffic information services. These services provide road users with helpful and timely information on things such as traffic regulations, driving routes, estimated travel times and potential delays to a journey. The public consultation aimed to gather stakeholders' views in an attempt to establish what problems there are with current services, identify opportunities for improvement and prepare specifications and standards for the future provision of these services. In our formal comments of 12 March 2014, we stressed that the collection and use of real-time traffic information may entail the processing of personal data. This is particularly relevant when dealing with equipment such as the eCall platform or GPS, where information is collected from users. We therefore recommended that the Commission should take EU data protection law fully into account when implementing any future specifications or legislation in this area, in particular Directive 95/46/EC and Directive 2002/58/EC. To do this, the Commission must ensure that privacy is embedded in the IT infrastructure and software at the design stage (privacy by design). There must also be appropriate safeguards governing the collection and re-use of location data and we reminded the Commission that the EDPS should be consulted prior to the adoption of any new specifications in this area.

3.4.3. Cross-border exchange of data on road traffic offences

The Commission requested the EDPS to provide comments on a proposal for a Directive facilitating cross-border exchange of information on road safety related to traffic offences. The proposed Directive replaces Directive 2011/82/EU, which was annulled by the Court of Justice of the European Union due to an incorrect legal basis, and aims at enacting a text almost identical to the first but with a correct legal basis (i.e. Article 91 TFEU on transport).

In our comments of 3 October 2014, we recalled that EDPS had issued an Opinion in 2008 on the original proposal. As some but not all of our recommendations had been taken into account in the final text, which is almost identical to the new one, we underlined that those recommendations were still valid. We welcomed that Directive 95/46/EC is mentioned as the applicable data protection law, and recalled that all processing activities involved should respect the obligations under Article 8 of the Charter, which must be interpreted in the light of more detailed rules such as those set forth in Directive 95/46/EC.

4. COOPERATION

Our strategic objective

Improve the good cooperation with Data Protection Authorities, in particular the Article 29 Working Party, to ensure greater consistency of data protection in the EU.

4.1. National data protection authorities

The Article 29 Data Protection Working Party (Article 29 Working Party) is an independent advisory body set up under Article 29 of Directive 95/46/EC. It is composed of representatives of the national data protection authorities, the EDPS and the Commission. It provides the European Commission with independent advice on data protection issues and contributes to the development of harmonised policies for data protection in EU Member States.

Cooperating with other data protection authorities in the EU is one of the core tasks of the EDPS, as laid down by Regulation (EC) No 45/2001. This includes participation in the activities of the Article 29 Working Party in order to ensure greater consistency of data protection in the EU.

Our advisory role to some degree coincides with the role given to the Working Party so we aim to ensure effective coordination with partner supervisory authorities. As a member, the EDPS contributes to the activities of the working party taking up a share of the work, comparable to the one taken up by other DPAs. However, this participation is based on a selective approach and focus where our contribution provides an added value, in particular in bringing an EU perspective, such as in the Working Party Opinion on legitimate interest, or the Opinion on open data. We were also closely involved in the opinions on device-fingerprinting, drones and on the internet of things.

4.2. Coordinated supervision

Direct cooperation with national authorities is an area of increasing importance in the context of the development of large-scale international databases such as Customs Information System (CIS), EURODAC, the Schengen Information System II (SIS II), the Visa Information System (VIS) or the Internal Market Information System (IMI), which require a coordinated approach to supervision. This cooperation work is in addition, but separate to our supervision work in this area (see chapter 2). In 2014, we provided the Secretariat for the supervision coordination groups of CIS[12], EURODAC[13], VIS[14], SIS II[15] and for the first time, the IMI[16]. In 2014, we organised nine meetings in total for all the coordinated supervision Groups (two for the CIS, two for EURODAC, one for the IMI, two for the SIS II and two for the VIS). Our role has included:

- Coordinating the meetings of all groups to ensure that they take place back-to-back in order to reduce the financial, travel and administrative burdens and to ensure consistent and horizontal supervision policies of those large-scale IT systems where possible.
- drafting and circulating relevant documents;
- liaison with members of the groups in between meetings to prepare business.

EURODAC is the large-scale IT system for the storage of the fingerprints of asylum seekers and persons apprehended irregularly crossing the external borders of the EU and several associated countries.[17]

12 For more information on CIS: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/SupervisionCoordination/CCIS

13 To read the EURODAC meeting reports: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/SupervisionCoordination/CEurodac

14 To read the VIS meeting reports: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/SupervisionCoordination/CVIS

15 For more information on SIS II: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/SupervisionCoordination/CSIS

16 To read the IMI meeting report: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/SupervisionCoordination/CIMIS

17 Iceland, Norway, Switzerland and Liechtenstein.

The Visa Information System (VIS) is a database containing information, including biometric data, on visa applications by third country nationals. This information is collected when a visa application is lodged at an EU consulate and used to prevent visa fraud and so-called visa-shopping between member states, to facilitate the identification of visa holders within the EU and to ensure that the visa applicant and the visa user are the same person. VIS was rolled out on a regional basis and first became operational in North Africa on 11 October 2011. VIS has since been implemented in fifteen other regions.[13]

The CIS Supervision Coordination Group is set up as a platform for the data protection authorities, responsible for the supervision of CIS in accordance with Regulation (EC) No 766/2008. The EDPS and national data protection authorities cooperate in line with their responsibilities in order to ensure coordinated supervision of CIS.

The Schengen information system (SIS) is a large scale IT system created following the abolition of controls at internal borders within the Schengen area. The SIS allows competent authorities in Member States to exchange information on performing checks on persons and objects at the external borders or on the territory, as well as for the issuance of visas and residence permits.

The SIS II Supervision Coordination Group is set up as a platform for the data protection authorities responsible for the supervision of SIS in accordance with Regulation (EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System and Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System. The EDPS and national data protection authorities cooperate in line with their responsibilities in order to ensure the coordinated supervision of the SIS.

18 http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/visa-information-system/index_en.htm.

4.3. European conference

Data Protection Authorities from member states of the European Union and of the Council of Europe meet annually for a spring conference to discuss matters of common interest and to exchange information and experience on different topics.

On 5 June 2014, the Council of Europe and the French 'Commission Nationale de l' Informatique et des Libertés' (CNIL) jointly organised the European Conference of Data Protection Authorities in Strasbourg.

The EDPS attends the annual conference as it is a unique opportunity for accredited data protection authorities and observers to deal with subjects of common interest and to help advance the fundamental right to data protection. The 2014 conference focused on ways for DPAs to cooperate better in the face of globalisation. A resolution was adopted which called on the Council of Europe, in its ongoing deliberations on modernising Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, to strengthen protection of individual rights, in particular through establishing independent supervisory authorities which are able to enforce and to cooperate with each other effectively.

4.4. International conference

Data Protection Authorities and Privacy Commissioners from Europe and other parts of the world, including Canada, Latin-America, Australia, New Zealand, Hong Kong, Japan and other jurisdictions in the Asia-Pacific region, have met annually for a conference in the autumn for many years.

The 2014 International Conference was organised by the Data Protection Office of Mauritius from 12 October to 16 October. This annual conference gathers public officials from international and sub-national authorities, as well as other experts in the field. It also brings together industry representatives and academics. The wide experience and knowledge of the participants provide a unique opportunity to discuss a large number of issues and challenges regarding different areas of data protection.

Several themes were on the agenda including, privacy and data protection in the developing world;

One Stop Shop: Centralisation versus Proximity; Surveillance versus Dataveillance; Privacy in the Digital Age – the UN General Assembly Resolution; eHealth and Data Protection; Ethics, Fundamental Rights and Big Data; and Net Neutrality and Data Protection. The Supervisor intervened in a workshop on accountability and a panel on 'privacy without territorial limits', and the Director spoke in a panel on net neutrality.

An important achievement of this conference was the adoption, in the closed session for data protection authorities (13-14 October), of the Arrangement and Resolution on international enforcement cooperation. This project has been under discussion for many years and we been very involved in supporting the negotiations. The rapid development of technologies such as cloud computing, big data and the internet of things (IOT) have underlined the need for a framework to enable data protection authorities to cooperate across borders.

The Supervisor also gave a short presentation at the closed session on the IPEN initiative (see section 7.2), which provoked great interest. The session was mainly devoted to a discussion on the internet of things. Research shows that at present, IoT devices tend not to respect data protection rules: they are often insecure, lack privacy notices, store personal data on the cloud, do not allow data subjects to have their data erased, and sell the data for profiling. These weaknesses have huge implications when IoT devices are combined with big data. The declaration on the internet of things was therefore another positive outcome of the conference.

The 2015 international conference will be organised by the Dutch Data Protection Authority, College bescherming persoonsgegevens, in Amsterdam at the end of October.

4.5. Non-EU countries, international organisations and privacy enforcement networks

In a hyper-connected world with evolving technologies and increasing exchanges of personal information, the protection of personal data requires global, coordinated and cross-border approaches.

We will continue not only to monitor technological developments and their impact on the protection of personal data, as required by Regulation 45/2001, but also to advise EU institutions and bodies as regards the protection of personal data when they negotiate international agreements or take positions in international fora.

We intervene selectively to ensure maximum impact with our limited resources. We therefore do most of this work by email and conference calls and attend a selection of key meetings of relevant regional and international fora.

We have continued to provide input on relevant documents discussed 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 international working group on data Protection in Telecommunications (Berlin Group) and the international conference of data protection and privacy commissioners.

We also attend their key meetings and participate as members or observers in the negotiations of the relevant binding and non-binding instruments they adopt.

On data protection developments in non-EU countries and privacy policies in international organisations (such as UNHCR), we try to monitor, provide advice and comments where necessary and possible, with the aim of ensuring that these countries or organisations, as potential recipients of data transferred under EU jurisdiction, provide as good a level of data protection as possible.

We will continue to engage in negotiations on the modernisation of Convention 108 to ensure that a good level of protection is ensured and that the text is compatible with the outcome of the EU data protection reform, to prevent EU member states from being subject to contradictory binding data protection instruments.

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

We have sought to ensure that relevant guidelines, recommendations, standards and other key texts negotiated at the OECD relating to the processing of personal data respect EU data protection principles and the principles agreed by the EDPS. Although most texts are not directly binding, they are often subsequently transposed into EU law and have a direct influence on other texts and debates at national, regional and international level.

We have worked 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.

In relation to proposals for a European working group on cooperation among data protection authorities, we have argued for consistency with the proposed cooperation mechanisms in the data protection package.

5. COURT CASES

One of the EDPS' more frequent tasks is intervening in cases before the Court of Justice of the EU (CJEU), the General Court and the Civil Service Tribunal.

Under Regulation (EC) No 45/2001, actions against the EDPS can be brought before the CJEU (Article 32), and so the EDPS acts as a defendant. For instance, EDPS decisions in complaint cases (see section 2.4) can be appealed before the CJEU. To date, three complainants have brought cases to court. The three cases were unsuccessful.

The EDPS may also refer alleged breaches of the provisions governing the processing of personal data under Article 47(1)(b), non-compliance with the exercise of the powers of the EDPS under Article 47(1)(c)-(f) and 47(2) (Article 47 (h)) (i.e. the EDPS as an applicant) to the CJEU. To date, neither has occurred.

In addition, the EDPS may intervene in actions brought before the CJEU (Article 47(1)). The right of the EDPS to intervene in actions before the court was recognised by the CJEU in the PNR cases (Cases C-317/04 and C-318/04, orders of 17 March 2005). The court based the right to intervene on the second subparagraph of Article 41(2) of Regulation (EC) No 45/2001 according to which the Supervisor is 'responsible for advising Community institutions and bodies on all matters concerning the processing of personal data'. This advisory task does not only cover the processing of personal data by those institutions or organs. The court interpreted the powers conferred on the EDPS by Article 47 of the Regulation in light of the purposes of Article 41.

In 2014, the EDPS intervened in several cases before the court:

- T-115/13 Dennekamp v Parliament (transparency/access to documents);

- T-343/13 CN v Parliament (publication of sensitive personal data on a website);

- C-615/13 P ClientEarth/PAN Europe (interpretation of the concept of personal data in the transparency/access to documents context and compliance with Article 8(b) of Regulation 45/2001, as well as the difference between the fundamental right to privacy and the fundamental right to personal data protection).

Article 41(2)-(4) of the EDPS Rules of Procedure lays down the criteria for considering an intervention. Those criteria include: whether the case is of general data protection importance or if the EDPS has been directly involved in the facts of the case in the performance of supervisory tasks; whether the data protection issue constitutes a substantial part of the case; and whether an intervention by the EDPS is likely to add value to the proceedings.

The interventions can be used in a strategic manner to address important or recurring problems (such as the broad concept of personal data under EU law), pursue a policy agenda (for example, in a series of transparency/access to documents related cases), and/or to present the EDPS approach to data protection issues (for instance, the distinction between Articles 7 and 8 of the Charter of Fundamental Rights).

6. ACCESS TO DOCUMENTS/ TRANSPARENCY

As an EU institution and according to its Rules of Procedure, the EDPS is also subject to the Public Access to Documents Regulation of 2001. The number of public access requests for documents held by the EDPS has increased progressively over the years. The number doubled in 2013 from 12 requests to 24. In 2014, we dealt with 18 requests, 4 of which were confirmatory applications to our initial replies.

The increasing number of cases we deal with in this field reveals the need for more detailed guidelines on the practical implementation of the Public Access Regulation. We are currently working on consolidating the methodology on how to deal with replies, according to the latest practice. In 2015, we will provide practical advice to the EU

institutions and bodies on how to balance transparency and the need for the protection of personal data in light of the Bavarian Lager ruling of the Court of Justice.

7. MONITORING TECHNOLOGY

Our strategic objective

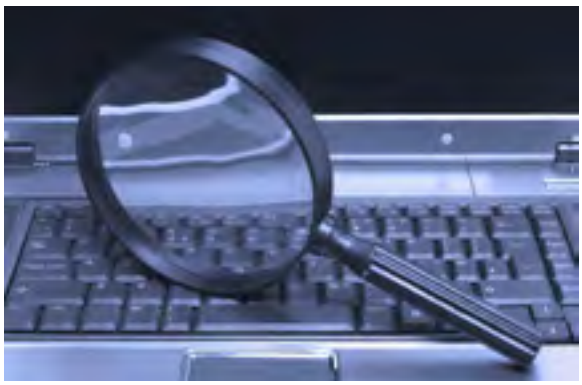
Assess the privacy risks of new technologies by collecting and analysing information as appropriate.

- *We provide guidance on technical aspects of data protection compliance to controllers. We also offer technical advice as part of specific guidelines.*
- *We continue to develop our technical supervision capabilities and use them in inspections and audits, as well as in cooperation with other data protection authorities in the context of Supervision Coordination Groups,*
- *We provide advice to the EU legislator on how to take account of the privacy effects of technology related initiatives and measures in policy and legislation.*
- *We promote the development of engineering practices which incorporate privacy concerns and encourage engineers to build privacy mechanisms into internet standards, services and apps through the Internet Privacy Engineering Network (IPEN).*
- *We actively engage and participate in a number of task force groups, technology sub-groups under the Article 29 Working Party, Commission working groups, standardisation initiatives and selected conferences to ensure that we are up-to-date on relevant data protection developments and best practices in technology.*
- *We apply data protection principles to our own internal IT issues, such as the hosting of the case management system.*

7.1. Technological development and data protection

7.1.1. Monitoring and reporting on technological development

In 2014, we strived to improve our continuous monitoring of technological developments, events and incidents and the assessment of their impact on data protection. This has enabled us to provide appropriate advice on technical matters, with regard to our supervision, consultation and cooperation activities. The EDPS reports on the developments in our regular publications, such as newsletters and



annual reports. The impact of the wider spread of connected mobile devices and a high number of security incidents were among the themes of 2014.

More and more devices are equipped with interfaces that allow transmission of the data they collect. Wearable devices such as sports monitors equipped with satellite navigation technology record biometric data, the location and movement of their user and transmit them to the servers of their manufacturers as soon as they are connected. Cars can record and transmit data about their functions, position and behaviour of their drivers.

There are concerns that security might not be keeping up with the increased collection and transmission of personal data. The number of serious security flaws discovered in widespread systems is also increasing: in 2014, it was found that some of the most popular mobile devices were vulnerable to interception of seemingly encrypted communications. It was also revealed that a piece of code found in many Linux systems had a flaw allowing attackers bypass security protections. A vulnerability was also discovered in smartphone operating systems where the chip responsible for the communication over the network could override all restrictions protecting the 'smart' part of the phone, and so gain access to all information stored on the smartphone.

In 2014, a number of security flaws in widely used systems found broad interest. Some of the vulnerabilities were given names like Heartbleed, Gotofail and Poodle. The Heartbleed bug[14] was discovered

14 CVE-2014-0160.

in OpenSSL, a popular encryption tool for internet communications. Heartbleed makes it possible to read and access data that should be protected.

Many popular internet services seemed to be vulnerable and appeared to take the necessary measures to quickly fix the bug on their systems. The European institutions also secured their services. Users of affected services were advised to change their passwords and the certificates used for encrypting internet traffic between affected websites were replaced. Yet despite all these measures, it is possible that there are servers which have not yet been updated and which are therefore still using the affected software.

7.1.2. IT Policy Laboratory

The EDPS IT Policy Laboratory was set up in 2014 with equipment and tools that can be used to assess the privacy features of certain products or systems used in the field of our supervision work.

The lab helps to assess the privacy effects of new technical developments in mobile device communications and to inspect the data protection compliance of websites; it may also be used for testing new or modified platforms with data protection relevance, such as results of university research projects or new industry products.

The IT lab is now operational and will be complemented by a mobile IT kit, in order to provide on-the-spot demonstrations, perform experiments and/or technical tests on site in the context of inspections and audits.

7.2. Promoting privacy engineering

7.2.1. The IPEN initiative

An important action point in the new EDPS strategy is the promotion of privacy friendly technology through cooperation with different stakeholders.

In 2014, we launched the Internet Privacy Engineering Network (IPEN) in collaboration with national data protection authorities (DPAs), developers and researchers from industry and academia and civil society. The initiative aims to develop engineering practices which incorporate privacy concerns and encourage engineers to build privacy mechanisms into internet standards, services and apps.

One reason for the lack of attention to privacy issues in development is the lack of appropriate tools and best practices. Developers have to deliver quickly in order to minimise the time and effort to market the output, and often re-use existing components, despite their privacy flaws. There are, unfortunately, few building blocks for privacy friendly applications and services and security can often be weak as well.

The purpose of IPEN is to close the gap between technical tools (guided by engineers and IT experts) and personal data protection needs (guided by the law) by encouraging the development of privacy friendly solutions for common engineering problems and enabling developers to recognise when their technical choices have an impact on privacy principles.

The first IPEN workshop took place on 26 September 2014 in Berlin and was organised together with several DPAs and other organisations. The workshop was designed to be a practical approach to identify privacy gaps in existing technology and develop useful solutions.

The theme of our debate was *How can we develop internet services and apps which respect users' privacy and personal data?* Workshop participants identified 10 lines of action to pursue.

Among the projects proposed was the creation of a 'data protection cookbook' for system development. Designed for IT developers, this project will include a manual with a step-by-step guide on how to incorporate privacy considerations into internet tools and development processes. Participants also recommended the creation of a 'business process design cookbook', to provide guidance to businesses to integrate data protection in their ways of working.

In addition, participants agreed on the necessity of finding ways to bridge the communication gap

between lawyers and engineers. It was agreed that greater understanding and cooperation between the two communities is essential to ensure that personal data protection is incorporated in the technology that we use on a daily basis.

Following the success of the first workshop, the IPEN initiative is now focused on developing and addressing the identified projects. IPEN will continue to explore ways to develop privacy-friendly technologies and to ensure that privacy becomes an essential consideration for all IT developers.

7.2.2. Intelligent Transport System

In November 2014, the European Commission launched its platform for cooperative intelligent transport systems (C-ITS). The EDPS participated in the kick-off meeting of the working group on Governance and Privacy. Cooperative Intelligent Transport Systems (C-ITS) is a group of technologies and applications that allow vehicles to become connected to each other and to other elements of the transport system, e.g. traffic control or toll collections systems. The working groups comprise experts from national authorities and the Commission as well as public and private organisations active in C-ITS, such as automobile clubs, car manufacturers, toll road operators and manufacturers of navigation systems and other car electronics.

At the working group on Governance and Privacy, we gave an overview of the applicable EU framework for data protection, as well as relevant elements of the reform. Privacy aspects are highly important to the deployment of C-ITS due to their potential to collect huge amounts of data such as location, vehicle model and identification number, speed or acceleration as well as the personal information of C-ITS users. This data could be used for profiling or tracking. The EDPS presentation built on our previous work in the domain, such as the Opinions and comments on eCall, digital tachographs and ITS. We will continue to follow this initiative in 2015.

7.3. Supervision

7.3.1. Guidelines on obligations in the field of information technology

To build on our capacity to give advice to controllers on technical measures for the effective implementation of data protection in IT systems, we have been developing guidelines for specific IT areas. The target audience includes controllers and the DPO community and also the IT departments of EU institutions.

The guidelines describe the legal obligations and outline recommendations and best practices. The guidelines will offer flexibility to the controller to follow our recommendations as useful and authoritative advice or take responsibility to choose another, equally effective, way to comply with the obligations. The guidelines will be available in the course of 2015.

7.3.2. Tor access to EU websites

The Tor network serves as a means for users to protect their internet communications against interception and surveillance. In 2012, we were made aware of the systematic blocking by some EU websites of all access from the Tor network[15]. While network security concerns were given as justification for this restrictive measure, we pointed out that the EU regulatory framework explicitly recognises anonymous communications, and that necessity and proportionality would need to be assessed properly. After these exchanges the relevant security policy was reviewed and Tor is no longer systematically blocked. Since then, the EDPS has verified on a number of occasions that the blocking of the Tor network is indeed no longer in effect, to the benefit of European and non-European citizens which want or need to protect their web browsing privacy.

7.4. Consultation

7.4.1. eu-Lisa

Given the scope of the responsibilities assigned to eu-LISA, the European agency for the operational management of large-scale IT Systems in the Area of Freedom, Security and Justice, we have kept a close eye on the developments of the agency and the large-scale IT systems under its purview (SIS II, VIS and Eurodac). In 2014, we visited eu-LISA's

15 From https://www.torproject.org/:*'Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security'.*

Tallinn premises in order to raise awareness on data protection-related matters and initiate discussions on IT and IT security management of the systems.

In line with the SIS II Regulation and as its supervisory authority, we also began our inspection of eu-LISA's Strasbourg site towards the end of 2014 in order to check the security and the operational management of the system used by border guards, customs officers, visa and law-enforcement authorities throughout the Schengen area. The inspection is expected to end in early 2015 with a report that will be circulated according to the provisions laid down in the SIS II Regulation.

We also continued to closely monitor technical developments on the smart borders package. Even though the package is still under discussion, eu-LISA has been tasked with launching a pilot project that would help the legislator better understand the intricacies of such an enterprise. In 2014, we had several meetings with the Commission and eu-LISA representatives in order to provide guidance on aspects of the pilot affecting the protection of personal data and we plan to remain involved in the practical implementation of this pilot in 2015.

7.5. Cooperation

7.5.1. Technology aspects of data protection

Our technology and IT policy expertise plays a valuable role in the EPDS' task of cooperating with other DPAs. In 2014, we participated in the:

- Technology, eGovernment and BTLE subgroups of the Article 29 Working Party, where we ensure the EDPS IT, policy and consultation contributions in the technology sub-group in terms of.
- International Working Group on Data Protection in Telecommunications (IWGDPT), also known as the 'Berlin group'.
- Expert groups coordinated by the Commission in the context of its technology related policies such as the Best Available Techniques (BAT) stakeholders' forum of the Smart Grid Task Force and the Commission's Enterprise and Industry Privacy by Design group for security industry.
- Comité Informatique Interinstitutionnel (CII) - both the general meetings and in the IT security subgroup - where the IT central departments of all EU institutions are represented.
- Cloud Virtual Task Force co-ordinated by the Commission's Directorate-General for Informatics (DIGIT) with a view to developing a DIGIT Cloud Strategy and the use of cloud services by EU institutions.

7.5.2. Smart policies for smart grids

Together with the Article 29 Working Party, we have been closely following the Commission's initiatives on the roll-out of smart grids, and have provided comments at different stages of the process. In 2014, the Commission proposed among other things a data protection impact assessment template.

The template is now in a test phase before being incorporated in a new Commission recommendation, which will define the context and terms for its review and revision. The template will also be accompanied by a document on Best Available Techniques (BAT), to which we are actively contributing through the work of the Smart Metering BAT Stakeholder Forum. In 2015, we will continue to offer support to the Commission on all matters related to smart meters and grids so as to ensure that viable solutions are found to mitigate all data protection risks.

7.5.3. Cloud services: for a step-by-step approach driven by management of risks and lessons learned

Many European institutions are already starting to use cloud services to support some of their tasks or are setting up public procurement with a view to such solutions.

Together with other European institutions, the Commission is developing an approach for the use of cloud computing in public administration. We are contributing to this effort as possible users of cloud computing services and to provide advice on the data protection requirements.

At the end of December 2014, the Commission published the first inter-institutional call for tenders for the EU institutions to procure cloud computing services to support low risk business processes, where no personal data or non-sensitive personal data are implicated.

In 2015, we will continue to support the EU institutions and finalise our guidelines on cloud computing which, given the rapid evolution of cloud services, will be a work in progress but should still provide clear operational principles and practical help.

7.5.4. The Berlin Group

The International Working Group on Data Protection in Telecommunications (IWGDPT, also known as the Berlin Group) is composed of data protection and privacy experts from Europe, America and Asia. As part of the working group, we participate in the meetings and contribute to the documents produced by the group which in 2014, included working papers on 'own devices' in corporate networks (BYOD) and on big data and privacy. The latter served as the basis for a resolution adopted at the 36th International Conference of Data Protection and Privacy Commissioners.

7.6. EDPS IT

We want to ensure that our internal IT operates effectively and efficiently while also being in line with data protection requirements. This objective requires continuous monitoring and improvement. The EDPS IT Steering Committee, chaired by the Head of IT Policy, controls this process within EDPS.

Additionally, the IT training needs of EDPS staff and programmes to fulfil them were identified in 2014. Informal tutorials, for example, on IP addresses as personal data, or structured presentations and discussions on specific topics, sometimes calling on external experts to speak, included the introduction to computer forensics and IT security requirements in the EU institutions.

7.7. EDPS website security

In the second half of 2014, we worked with the technical team in the European Parliament to improve the security of our website. Thanks to the collaboration, effort and expertise of both parties, our webpages are now encrypted under the most stringent standards avoiding the most serious known weaknesses[16]. We will continue to work on improving security and related processes in 2015.

7.8. EDPS Case Management System

The EDPS case management system (CMS) has been operational since October 2013 and is used by all staff as a central repository for EDPS case documents. A position of records manager/archivist was created within the IT Policy team, also incorporating the function of CMS business administrator, who provides second-level support to staff.

A small network of 'super-users' within each team offers first level support to other colleagues. The super-users give feedback to the CMS business administrator about the functioning of the system and help identify potential changes. The system is regularly adapted to new requirements and its functionality is extended in order to optimise support for EDPS operations and business needs.

16 Rating confirmed at the moment of publication: https://www.ssllabs.com/ssltest/analyze.html?d=secure.edps.europa.eu.

8. INFORMATION AND COMMUNICATION

Our strategic objective

Develop a creative and an effective communication strategy.

8.1. The EDPS as a point of reference

Information and communication activities play a significant role in raising awareness of the EDPS, mandate, policies and decisions. Our activities target the EU administration and the wider public and we use tools and activities such as press releases, publications, events, tweets and our website to reach out to them. Our audiences have varying degrees of knowledge on the topic of data protection and we therefore tailor our approach to their differing needs.

The EDPS aims to be a point of reference in the EU for data protection and privacy. Evidence such as the number of press and information requests and media and social media coverage suggest that we continue to consolidate this position.

2014 might be described as a year of transition for the EDPS, as it should have marked the beginning of a new mandate; the new appointments did not in fact happen until the end of the year. The delayed selection and appointment of a new Supervisor and Assistant EDPS had an impact on our information and communication activities: while we continued to deliver our remit, no significant new activities were undertaken in the interim period.

8.2. Communication features

Our main stakeholders are the EU institutions and bodies that we supervise. EDPS messages are therefore largely tailored to EU staff, but include other target groups including the wider public, EU political stakeholders and those in the data protection community.

Though our communication policy does not need to engage in mass communication, we do employ a range of tools to communicate with the general public. These include our website, Twitter, publications, awareness-raising events and regular interaction with interested parties.

8.2.1. Language policy

We tailor our communication style to communicate the same message to different audiences. For example, to non-experts data protection can often seem technical and obscure, so we use straightforward language and avoid jargon to make it accessible. However, when addressing more informed audiences, we are able to use more specialised language. In addition, we offer our press and communications activities in at least three languages - English, French and German.

8.3. Media relations

We frequently interact with the media through press releases, interviews and press events to promote the EDPS as an independent point of reference for data protection in the EU. Our interactions with the press have allowed us to develop and maintain our already impressive list of media contacts.

8.3.1. Press releases

The EDPS issued 14 press releases and statements in 2014, all of which were published on the EDPS and EU Newsroom websites. These press releases and statements addressed topics such as the EU

data protection reform, big data, the area of freedom, security and justice, IPEN, financial services markets and conflicts of interest.

Press releases are distributed to our network of journalists and interested parties and our monitoring of the media shows that these frequently result in significant coverage in general and specialised media outlets. Additionally, our press releases are often published on institutional and non-institutional websites, from EU institutions and bodies, to civil liberty groups, academics institutions, information technology firms and others.

8.3.2. Press conferences, interviews and media enquiries

On 1 April 2014, we held a press conference to present our Annual Report for 2013, at which the Supervisors also answered questions from journalists on the data protection reform package. It was a well-attended conference and received widespread coverage in the EU press.

In addition to this, the EDPS and Assistant EDPS gave 42 direct interviews to European and international journalists from print, broadcast and electronic media during 2014. The EDPS also received 38 written media enquiries, addressing a range of issues including big data, the right to be forgotten and data retention.

8.4. Requests for information and advice

We received 132 requests for information and assistance in 2014. This is a decrease from 2013 (176), suggesting that we are becoming increasingly effective in communicating our messages.

The majority of these enquiries came from individuals who asked for more information on privacy matters or assistance in dealing with problems such as the security or misuse of their personal information. We also received enquiries from staff in the EU institutions, layers and law firms, private companies and industry associations and students and NGOs.

Many of the requests received in 2014 related to matters over which the EDPS has no competence. We responded to all of these enquiries, outlining the competencies of the EDPS and referring them to the relevant authority.

8.5. Study visits

Study visits help to increase awareness of data protection. In 2014, we accepted the requests of 7 groups, the majority of which comprised students and academics from the EU and US. Most were interested in the mandate and activities of the EDPS, the EU data protection reform and EU-US privacy relations.

8.6. Online information tools

8.6.1. Website

As our most important communication channel, the website is updated on a daily basis. Our website includes access to our Opinions on prior checks and on proposals for EU legislation, work priorities, publications, speeches of the Supervisor and Assistant Supervisor, press releases, newsletters and event information.

An analysis of traffic and navigation data shows that in 2014, we had a total of 70 937 new visitors to our website. This represents a decrease from 2013 (136 293). Similarly, the total number of website visits in 2014 was 194 637, a decrease from 293 029 in 2013. A plausible explanation for this is that 2014 was a year of transition for the EDPS and while we continued to deliver our remit, there were fewer new activities to report.

After the homepage, the most frequently viewed pages were news, consultation, press releases and supervision. Most visitors access the website via a link from another site, such as the Europa portal or our Wikipedia pages.

8.6.2. Newsletter

The EDPS newsletter is a valuable tool for informing readers of our most recent activities. Our

newsletters are available in English, French and German on our website and readers are included on our mailing list via an online subscription feature.

We published three issues of our newsletter in 2014, in the months of April, July and October. The number of subscribers rose from 1950 at the end of 2013, to 2373 at the end of 2014 and includes members of the European Parliament, staff members from the EU institutions, staff of national data protection authorities, journalists, the academic community, telecommunication companies and law firms.

8.6.3. Twitter

The EDPS has been a part of the Twitter community (@EU_EDPS) since 1 June 2012. Our Twitter policy, published on our website, reflects our step-by-step approach to maintain a contemporary information and communication tool that is manageable with limited resources. By the end of 2014, the EDPS had 2000 followers and had tweeted 434 times.

In line with our policy, our Tweets have centred on our press releases, new Opinions, new publications, speeches, articles and presentations, videos and upcoming participation in events.

8.6.4. LinkedIn

At the end of 2013, the EDPS took ownership of the LinkedIn page created automatically for us by the company. This has allowed us to update it and maintain a professional image on the site. The page is another avenue to promote the EDPS as an institution, strengthen our online presence and enhance our visibility. By the end of 2014, we had 297 followers.

8.7. Publications

8.7.1. Annual Report

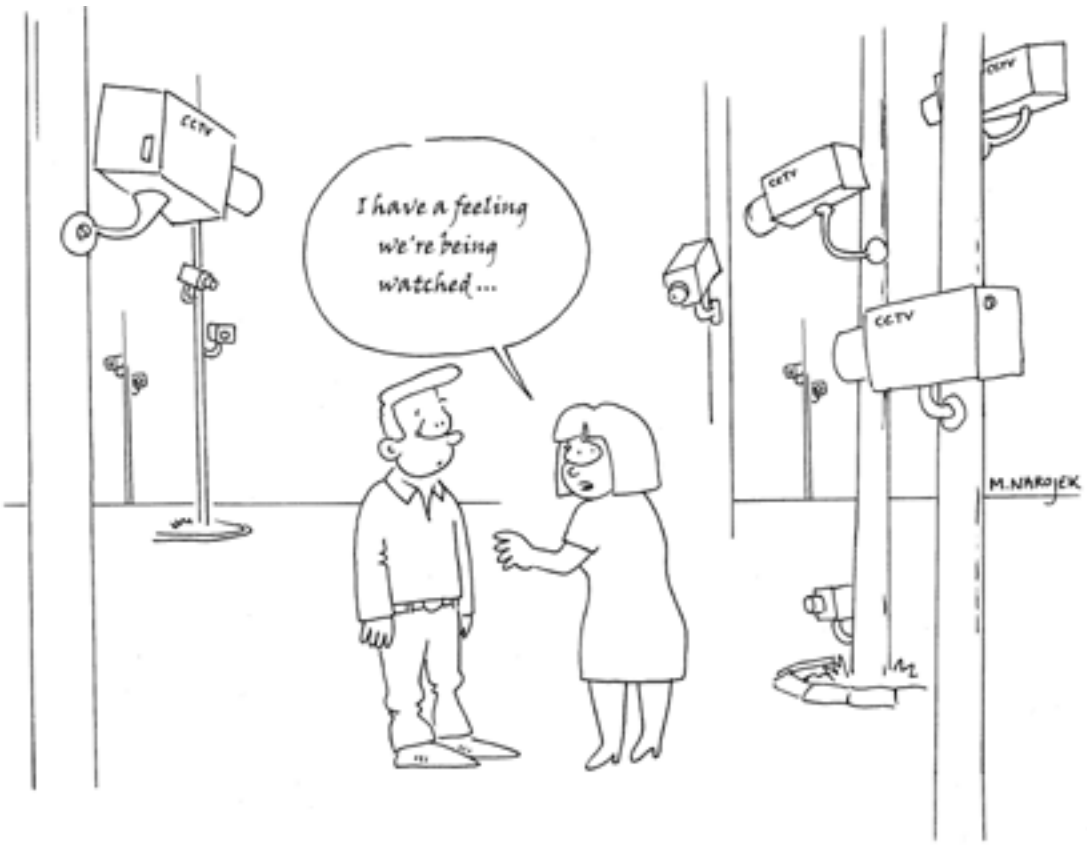
The EDPS annual report is an overview of our work in the main operational fields of supervision, consultation, cooperation and IT developments from the reporting year. It also sets out the main priorities for the following year.

Feedback suggests that the report is of interest to groups and individuals, experts and non-experts at international, European and national level who want more information on the protection of personal information in the EU.

The Supervisor and Assistant Supervisor presented our 2013 Annual Report to the LIBE Committee in the European Parliament on 1 April 2014. The main features of the report were also presented at a press conference on the same day (see 8.3.2).

8.8. Awareness-raising events

We look for opportunities that allow us to highlight the increasing relevance of privacy and data protection and to raise awareness of the rights of individuals as well as the obligations of the European administration.



8.8.1. Data Protection Day 2014

On 28 January 2014, 47 countries of the Council of Europe as well as European institutions, agencies and bodies celebrated the eighth European Data Protection Day. This date marks the anniversary of the Council of Europe Convention 108 on the protection of personal information, the first legally binding international instrument related to the field of data protection.

We use the opportunity to raise awareness among EU staff of data protection rights and obligations, either through our own events or alongside the DPOs of the EU institutions.

As part of our awareness raising efforts in 2014, we published a short video on our website as an entertaining and informative way to highlight some of the data protection rights and risks that are inherent in our everyday lives.

8.8.2. EU Open Day 2014

On Saturday 17 May 2014, we participated in the annual Open Day of the European institutions in Brussels, which also marks the anniversary of the Schuman Declaration. The EU Open Day is an excellent opportunity for us to increase general public awareness of data protection and the role of the EDPS.

Our 2014 stand, located in the European Parliament, proved hugely successful, with EDPS staff on hand to answer visitors' questions. Visitors could also take part in our data protection quiz and take away some information and promotional material. Two attractions on our stand were particularly popular. The first of these was a facial detection tool which identified the age and sex of a person through their facial features. The second was a web tracking application that visitors could use to see how much of their online activity is tracked when surfing the internet.

9. ADMINISTRATION, BUDGET AND STAFF

Our strategic objective

Improve the use of EDPS human, financial, technical and organisational resources.

9.1. Introduction

2014 was a transition year for the EDPS due to the Commission re-launching the selection procedure for a new team of Supervisors. The uncertainties surrounding the appointment of the new Supervisor and Assistant Supervisor also presented considerable HR and management challenges.

The entry into force of the new Staff Regulations for EU officials made it necessary to review many of our administrative decisions. The process of drafting and consulting both management and the Staff Committee on 19 implementing measures was time consuming and demanding for our small HR team.

In 2014, we continued to improve the strategic management of our human and financial resources, delivering a very high budget implementation rate and internal redeployments to maximise the use of our limited resources. We also adopted three important HR policy documents: a new code of good conduct, a DNA paper, reflecting on the organisational culture of the EDPS and a document on best practices for internal communication.

Further to the publication of a call for interest for officials in other EU institutions, we organised, with the invaluable assistance of the European Personnel Selection Office, an EU competition for administrators (AD 6) in the field of data protection. This will result in a reserve list of highly qualified data protection experts, as of the second half of 2015.

9.2. Budget, finance and procurement

9.2.1. Budget

The allocated budget for the EDPS in 2014 was EUR 8 018 796, which represents an increase of 4.66% on the 2013 budget.

In 2014, we remained fully committed to the EU's policy of austerity and budget consolidation, and strictly followed the orientations proposed by the Commission. Our approach also had to take into account the costs associated with the beginning of the mandate of two new members.

The delay in the selection procedure for a new team of Supervisors meant that Mr. Hustinx and Mr. Buttarelli had to stay in office until the end of 2014. As it was not possible to use the credits allocated in the budget to cover their allowances for the temporary extension period, an amending budget to return the corresponding unused credits (EUR 248 460) to the general EU budget was introduced in June 2014.

Despite these extraordinary appropriations, we implemented the austerity policy by reducing or freezing a large majority of our credits to 0% for the third year and carrying out substantial cuts to key budget lines such as translations (-17%), publications (-25%) and activities of the institutions (-17%).

Quarterly reviews of the implementation of our budget have led to better implementation rates:

from 76.9% in 2011 to around 92% expected for 2014.

9.2.2. Finance

There were no concerns or recommendations to be addressed by us in the Statement of Assurance from the Court of Auditors for the financial year 2013 (DAS 2013).

The Commission continued to assist us in finance matters in 2014, particularly in relation to accountancy services, as the Accounting Officer of the Commission is also the Accounting Officer of the EDPS.

Following the IAS recommendations and according to the EDPS Strategic Internal Audit Plan, the EDPS Internal Guide to Financial Transactions was updated.

9.2.3. Procurement

Further to the IAS recommendations and according to the EDPS Strategic Internal Audit Plan, a Procurement Plan was adopted for the first time for the year 2014.

In order to address our communication and video production needs, a low value procurement procedure was launched in 2014.

As part of our drive towards greater autonomy, we began to engage in the inter-institutional process for calls for tender. This has allowed us to make specific contracts directly with the companies rather than rely on larger institutions. The majority of the calls for tender of interest to us are in technical and IT related fields.

9.3. Human resources

9.3.1. Recruitment

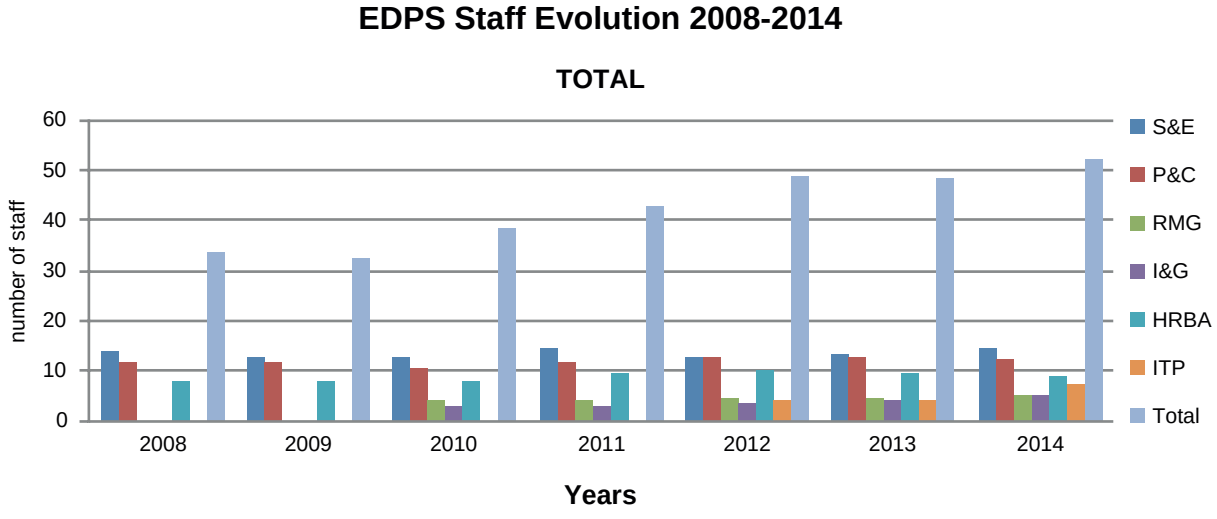
Officials are recruited either from other European institutions through inter-institutional transfers, from reserve lists of laureates of EPSO general competitions or from a list of laureates of a data protection competition organised by EPSO for the EDPS in 2009. As this was almost exhausted and in order to cope with future needs, a new specialist data protection competition was organised by EPSO in 2014.

In 2014, we recruited five EU officials, five contract agents and a seconded national expert.

The chart below shows a slight increase in our number of staff compared with the previous two years.

9.3.2. Our visibility in the EU market place: call for interest in other EU institutions

In order to tackle a relatively high turn-over combined with a few transfer requests from other EU institutions, we launched a call for expression of interest for EU officials interested in working for the EDPS in February 2014. The purpose of this soft call for interest was both to increase the visibility of the EDPS as an employer and to secure enough candidates to cope with the turn-over of staff.



The call for interest triggered a lot of reaction from officials and non-officials. 68 of these had profiles that were eligible, two of whom were recruited in 2014.

9.3.3. Professionalising the HR function

In line with the Commission HR programme of professionalisation, and our third annual HR report to the EDPS Management Board in February 2014, an action plan was implemented in 2014 that also addressed the issues raised in our 2013 survey on staff engagement, such as internal communication and working conditions.

9.3.4. Traineeship programme

Traineeships at the EDPS offer practical experience in our day-to-day activities in the operational and horizontal units. The programme hosts on average four to seven trainees per session (two five-month sessions per year). In 2014, there were 12 remunerated trainees in total at the EDPS.

9.3.5. Programme for seconded national experts

On average, we recruit one or two national experts from DPAs every year. These secondments allow us to benefit from the skills and experience of such staff and help increase our visibility in the member states. This programme, in turn, allows SNEs to familiarise themselves with data protection issues at EU level.

In 2014, the secondment of the national expert from the UK Data Protection Authority (ICO) came to an end and a new national expert from Sweden was recruited in May.

9.3.6. New staff regulations and implementing measures

The new Staff Regulations that came into force on 1 January 2014 made it necessary to update our Human Resource and Administrative decisions.

In 2014, in close cooperation with the EDPS Staff Committee, the HR team reviewed these internal decisions (appraisal, promotion, leave management, working conditions, etc.) and our AIPN adopted 19 decisions in total. The involvement and support of the Staff Committee of the EDPS was remarkable and where possible, we aligned our practices with those of the European Commission.

9.3.7. Update of recruitment manuals

Following the IAS global risk assessment at the end of 2013, we updated our manuals for selection and recruitment according to their recommendations. Furthermore, to prepare for a Court of Auditor's audit in 2015-2016, we also updated the appraisal decision and established a clear list of delegations.

9.3.8. New Code of Conduct and DNA paper

In June 2014, we adopted a new Code of Good Conduct, replacing the one from 2006. In December, we also adopted a DNA paper reflecting on the organisational culture of the EDPS. Both documents were included in the welcome package for the new team of Supervisors and are part of the welcome package for new staff.

9.3.9. Internal communication paper

Good internal communication practices are essential to maintain a good organisational climate, efficiency and high levels of staff engagement. Good

communication between representatives of the staff committee and management is also vital. A task force on internal communication established in the second half of 2014 drafted a paper on best practices which was adopted on 9 December 2014.

9.3.10. Learning and development

A new strategy: In 2014, we launched a new strategy for Learning and Development at the EDPS. The main principle of this strategy is to move from 'delivery of training' to 'support for learning'. The strategy aims to strike a balance between classic classroom training and different ways of developing personal skills and competencies. 2014 was a transition year in phasing out the old and phasing in the new strategy.

Short secondment and exchange programme: The aim of the EDPS short secondments and exchanges programme is to offer another avenue for staff development, career opportunities, increase staff motivation and engagement while strengthening the links with our stakeholders and key partner organisations.

Two pilot projects in November 2014 helped us assess the feasibility of the programme. The overwhelmingly positive outcome of both pilots means that we will officially launch the programme in early 2015.

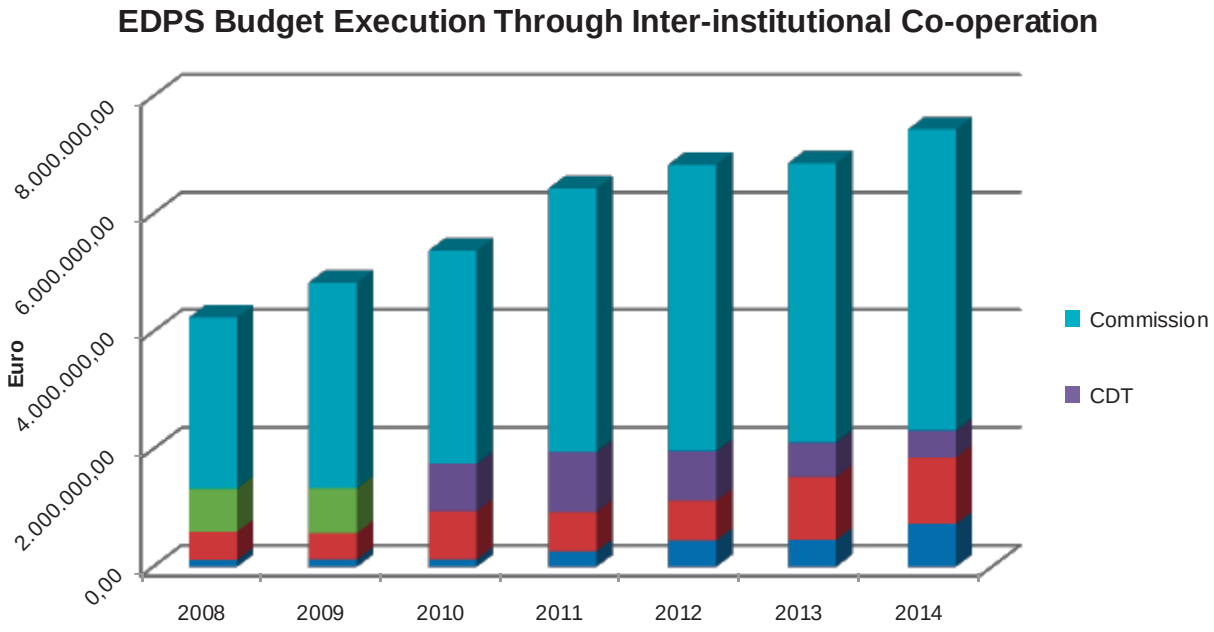
Some data on L&D: The Key Performance Indicator set to measure the rate of training implementation in 2014 was achieved and exceeded that of 2013. In 2014, the rate of implementation was 87,4%.

9.4. Administrative environment

9.4.1. Administrative assistance and inter-institutional cooperation

The EDPS benefits from inter-institutional cooperation in many areas by virtue of Service Level Agreements with the Commission and a cooperation agreement with the Parliament. This administrative cooperation is vital for us as it increases efficiency and allows for economies of scale.

In 2014, we adopted a new security decision (EUCI) and continued our close cooperation with various Commission Directorates-General (Personnel and Administration, Budget, Internal Audit Service, Infrastructure and Logistics, Education and Culture), the Paymaster's Office (PMO); the European School of Administration (EUSA); and the Translation Centre for the Bodies of the European Union. This cooperation takes place by means of service level agreements, which are updated regularly.



10. EDPS DATA PROTECTION OFFICER

10.1. The DPO at the EDPS

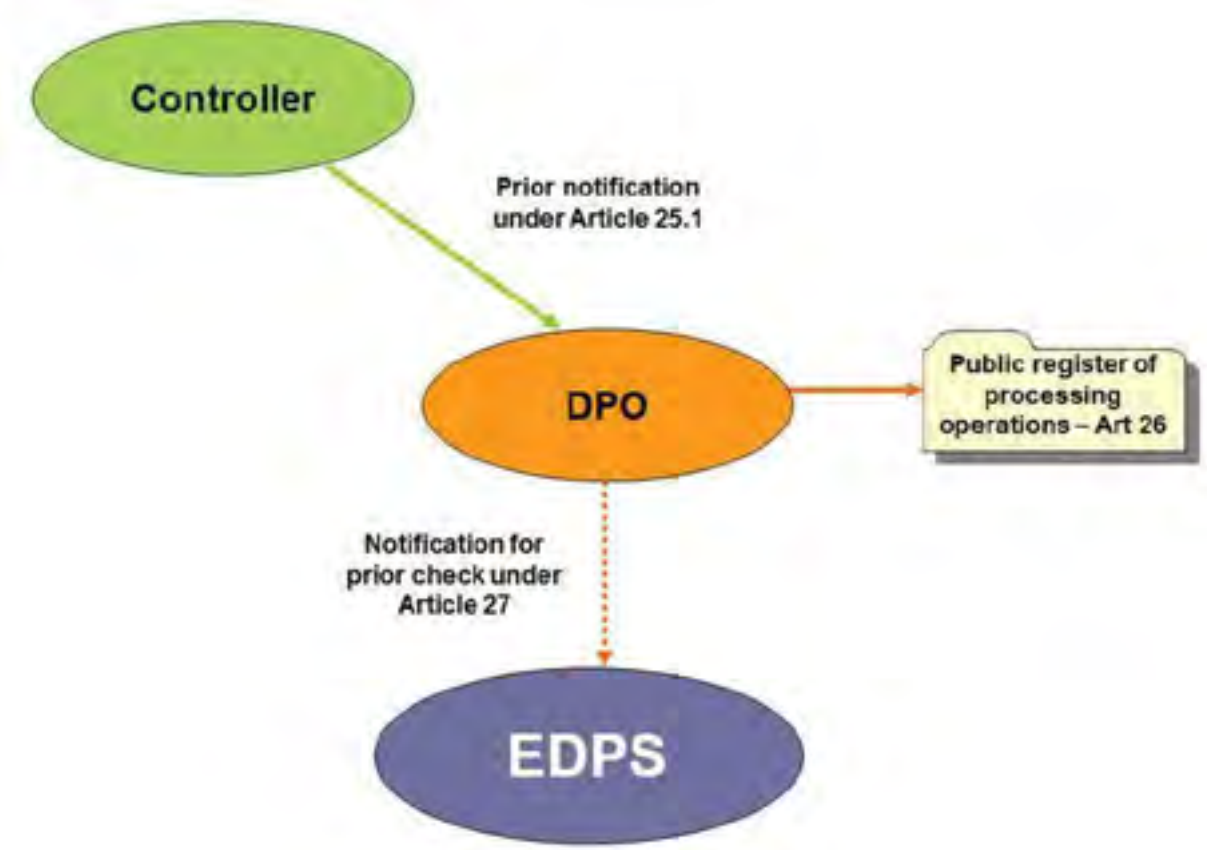
The role of the data protection officer (DPO) at the EDPS presents many challenges: being independent within an independent institution, meeting the expectations of colleagues who are specialist in data protection issues and delivering solutions that can serve as benchmarks for other institutions.

In October 2014, a new DPO team replaced the former DPO. In line with the motto of the new EDPS mandate of leading by example, the DPO team plans to trigger new synergies and projects so that the EDPS goes beyond compliance towards accountability in the years to come.

10.2. The Register of processing operations

Under Article 26 of the Regulation, the DPO must keep a register of all processing operations for which they have been notified. The register includes all relevant processing operations within the institution and lists each notification relating to those processing operations.

In 2014, the DPO team began to revise the register of existing notifications. In 2015, they will continue this work and focus their attention on the implications of the use of technologies and technological changes with regard to Regulation 45/2001.



10.3. Information and raising awareness

The DPO attaches great importance to raising the awareness of staff involved in processing operations and to the communication of data protection compliance at the EDPS. Part of the external communication activities at the EDPS in which the DPO is involved is the dedicated DPO section on the EDPS website which offers information about the DPO's role and activities and is updated regularly so that the updated register and all notifications are available for public consultation.

The DPOs of the EU institutions and bodies meet at regular intervals to share experiences and discuss relevant issues. As part of this productive network, the DPO team participated in the DPO network meetings in Brussels in June 2014 and Thessaloniki in November 2014. These meetings represent a unique opportunity to network, discuss common concerns and share best practice.

The EDPS intranet provides an effective means of internal communication with staff. The DPO intranet section contains information that is useful for staff: the main elements of the role of the DPO, the implementing rules, the DPO Action Plan and information on DPO activities. The DPO intranet section also contains a detailed list of privacy statements with all the relevant details (relating to Articles 11 and 12 of Regulation 45/2001) of EDPS processing operations, allowing staff to stay informed and be able exercise their rights.

The DPO also raises awareness by regularly presenting an Initiation to Regulation 45/2001 session to newcomers, trainees and officials who may not be experts in data protection. The purpose is to familiarise new staff with our data protection mission and values. The meetings are tailored according to staff expertise and role at the EDPS. A new element to this presentation focused on the role and work of DPOs is being developed.

11. MAIN OBJECTIVES FOR 2015

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

11.1. Supervision and enforcement

In 2015, we will continue to promote the accountability of EU bodies when they process personal data.

• Library of experience

Utilising our ten years of experience in applying Regulation 45/2001, we will develop an internal repository of our case law to ensure that our valuable expertise is catalogued;

• Regulation 45/2001

Relying on this solid experience, we will work with the European Parliament, Council and Commission to ensure that the existing rules set out in Regulation 45/2001 are brought into line with the General Data Protection Regulation.

• Training & interaction

We will continue to train and guide EU bodies on how best to respect data protection rules in practice, focusing our efforts on those types of processing which present high risks to individuals. We will maintain our close interaction with EU bodies, offering them relevant expertise and advice, which in turn will help us to strengthen our practical knowledge of their reality.

• DPOs

In close cooperation with data protection officers, we will continue to support EU institutions in moving beyond a purely compliance-based approach to one that is also based on accountability. In particular, we will work with them to develop data privacy impact assessments and data breach notifications.

• Coordinated Supervision

We will continue to supervise large scale IT systems in close cooperation with the national data protection authorities;

• **Inspections**

We will improve our methodology for inspections and visits, in particular a more streamlined method for inspecting IT systems.

11.2. Policy and consultation

As part of the delivery of the EDPS Strategy for 2015-2019, five key areas have been identified for our policy and consultation work in 2015:

• **Big data and the digital single market**

We will present a vision for how the EU should ensure individuals are able to exercise user control, enjoy the benefits of big data and ensure organisations and businesses are transparent and accountable for the personal data processing for which they are responsible. We will elaborate the vibrant debate stimulated by our Preliminary Opinion on competition law, consumer protection, privacy and the digital economy by participating in events and discussion with regulators.

• **Finalising the reform of the data protection framework**

Before summer 2015, we will present a policy briefing for the institutions to inform and help find practical and flexible solutions during the forthcoming trilogue on the General Data Protection Regulation and the Directive on data protection in law enforcement cooperation. We will also turn our focus, in close cooperation with national supervisory authorities, to implementation of the new rules. In particular, we will help prepare for a seamless transition to the new European Data Protection Board (EDPB), without prejudice to the co-legislators' future decision on the organisation of the Board's secretariat. We will engage in the early stage policy discussion on the development of implementing sector specific legislation, such as any proposal to reform Directive 2002/58/EC.

• **International agreements**

We will work proactively with EU institutions to ensure data protection principles are properly and consistently taken into consideration when negotiating international agreements on trade as well as law enforcement, such as TTIP, TISA and Safe Harbour and the scheduled automatic renewal of the TFTP agreement with the US. We will also offer our expertise and assistance where appropriate in the monitoring of existing agreements, such as the bilateral agreements on PNR.

• **Equipping policymakers in the home affairs sector**

In liaison with experts from the Commission, we aim to prepare guidelines on integrating data protection rules and principles in proposals and policies on internal security, border management and migration. The new European Agenda on Security needs to include more convergence between different data protection laws in this area and consistency in the supervision of large-scale IT systems. On specific measures, such as an EU PNR directive and the 'Smart Borders' package where discussions are ongoing, we have offered to work with the institutions to find ways to minimise intrusiveness into the rights to privacy and to data protection of the vast number of individuals potentially affected. Our advice will be predicated on recent case law especially the CJEU judgment on the Data Retention Directive in Digital Rights Ireland. We will also prepare a background paper developing the concepts of necessity and proportionality, especially in the light of recent case law, and how they should be applied to proposals which have an impact on data protection.

• **Agreeing working methods with the EU institutions and bodies**

As announced in our Policy Paper, we will seek to agree efficient ways of working with the institutions, where appropriate through memoranda of understanding, in discharging our policy and consultation role. We will seek feedback on the value of our advice. This will build on recent close cooperation with the Italian presidency on a draft directive on the automatic exchange of bank account information between tax authorities. We will continue to liaise closely with the Fundamental Rights Agency on issues of common concern.

11.3. Cooperation

Our ambition is for the EU to speak with a single voice on questions of privacy and data protection. Therefore the central motor of our strategy will be close cooperation with fellow data protection authorities (DPAs).

• **Coordinated supervision**

We will continue to prioritise efficient and loyal engagement and support in the coordinated

supervision of CIS, EURODAC, IMI, SIS II and VIS. Our aim is to move to a more consolidated and effective governance model for systems under the former 'third pillar'.

• Article 29 Working Party

We will engage closely with the Working Party not only to ensure a smooth transition to the EDPB, but also in developing and contributing to policy opinions both in subgroup and in plenary meetings, as rapporteur where appropriate, and in the operational supervision of EU agencies and IT systems.

• Non EU countries and international organisations

We will promote a global alliance with data protection and privacy authorities to identify technical and regulatory responses to key challenges to data protection such as big data, the internet of things and mass surveillance. We will also be fully involved in discussions on data protection and privacy at international fora including the Council of Europe and the OECD.

11.4. IT Policy

• Data protection going digital

One of our key actions to achieve this strategic objective will be to improve our cooperation with stakeholders, particularly the technical community, in order to intensify interdisciplinary cooperation on data protection by design and by default.

• Internet Privacy Engineering Network

We will continue to focus on data protection and privacy from an engineering perspective. The distinguishing feature of IPEN is that it includes technology experts from DPAs, industry, academia and civil society, allowing it to focus its efforts on issues of practical relevance. In 2015, the network will expand and continue to work on lines of action established in 2014.

• Technology monitoring

Our technology monitoring activities will become more visible and made accessible to other stakeholders to inform their work. In addition to

informing our own activities, the cooperation with DPAs and with technology-oriented expert groups at EU-level, we will make our reports accessible to the public.

• Guidance on technology and data protection

In order to promote a data protection culture in the EU institutions supervised by the EDPS, the preparation of guidelines for specific technical areas, such as mobile devices, web services and cloud computing, will be concluded in 2015, complemented by guidance on specific areas such as risk management.

• IT security

The importance of IT security management has increased over the years. We will continue to develop our expertise in IT security and its systematic application as a supervisory authority in our inspection and auditing activities and as a partner in our cooperation with the IT security community, with particular focus on the EU Institutions.

11.5. Other fields

Information and communication

2015 is a year of change at the EDPS. With a new mandate and strategy, there is an atmosphere of anticipation and potential of what can be achieved over the next five years. As a reflection of this, there are several major information and communication projects that will be undertaken. Among them are:

• A new visual identity

A significant project for 2015 will be the revision of our visual identity which will entail a new logo and graphic chart. The knock on effect of the change in our visual identity is that all EDPS communication materials will also need to be updated (such as promotional items, publications, website and so on). Therefore, this will be a long-term project as we will continue to use the materials we have and update them when we run out or when it is no longer feasible to continue doing so.

• Updating the EDPS website

We will also be making some major technical updates to our website and we will use the opportunity to refresh the look and feel of it.

• Clear language

We have continued to make huge strides towards our clear language goal over the last few years. Our overriding aim is to correct the excessive legal and technical image of data protection. This remains a priority and so in 2015, we will continue our use of straightforward language to make technical issues more accessible, with examples that the general public can identify with.

Resource management and professionalising the HR function

The new EDPS mandate and strategy will entail changes that will impact our HR work and put additional pressure on a shrinking budget following several years of austerity policies.

- Among those changes, the likely adoption of a new Data Protection Regulation, replacing Directive 95/46/EC, may directly impact the organisational structure of the EDPS, particularly if, as provided in the Commission's proposal, the EDPS is entrusted with the provision of the Secretariat of the new European Data Protection Board (EDPB). Consequently, the budget for 2015 already includes a new Title III called the EDPB and an EDPB Task Force will be established in the second half of the year.

- In 2015, we will develop two papers that look at ways of increasing the accountability and ethical dimension of our institution: a new code of conduct for the team of Supervisors and a whistleblowing policy, further to the recommendations by the European Ombudsman.

- In our aim of leading by example, we will cooperate very closely with the EDPS DPO on a privacy impact assessment and the revision of data protection notifications further to the entry into force of the new Staff Regulations.

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.[17]

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,

17 OJ L 8, 12.1.2001, p. 1.

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 2.2).

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. These supervisory activities are discussed at greater length in Chapter 2 of this report.

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. These consultative activities of the EDPS are more widely discussed in Chapter 3 of this report, while technological issues are specifically covered in Chapter 5.

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. This cooperation, including developments in coordinated supervision, is further dealt with in Chapter 4 of this report.

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 — List of abbreviations

ACTA	Anti-Counterfeiting Trade Agreement
CIS	Customs Information System
CoA	Court of Auditors
CoR	Committee of the Regions
CPAS	*Comité de Préparation pour les Affaires Sociales*
DAS	Declaration of Assurance
DG INFSO	Directorate General for the Information Society and Media
DG MARKT	Internal Market and Services Directorate General
DIGIT	Directorate General Informatics
DPA	Data Protection Authority
DPC	Data Protection Coordinator
DPO	Data Protection Officer
EAS	European Administrative School
EASA	European Aviation Safety Agency
EC	European Communities
ECB	European Central Bank
ECDC	European Centre for Disease Prevention and Control
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EEA	European Environment Agency
EFSA	European Food Safety Authority
EIB	European Investment Bank
EIO	European Investigation Order
ENISA	European Network and Information Security Agency
ECHR	European Convention on Human Rights
EPO	European Protection Order
EPSO	European Personnel Selection Office
ERCEA	European Research Council Executive Agency
EU	European Union
EWRS	Early Warning Response System
FRA	European Union Agency for Fundamental Rights
HR	Human resources
IAS	Internal Auditing Service
ICT	Information and Communication Technology
IMI	Internal Market Information System
IOM	International Organisation for Migration
ISS	Internal Security Strategy
IT	Information technology
JRC	Joint Research Centre
JRO	Joint return operation
JSA	Joint Supervisory Authority
JSB	Joint Supervisory Body
JSIMC	Joint Sickness Insurance Management Committee
LIBE	European Parliament's Committee on Civil Liberties, Justice and Home Affairs
LISO	Local Information Security Officer
LSO	Local Security Officer
OHIM	Office for Harmonization in the Internal Market
OLAF	European Anti-fraud Office
PNR	Passenger Name Record

RFID	Radio Frequency Identification
SIS	Schengen Information System
SNE	Seconded national expert
SOC	Service and Operational Centre
s-TESTA	Secure Trans-European Services for Telematics between Administrations
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFTP	Terrorist Finance Tracking Programme
TFTS	Terrorist Finance Tracking System
TFUE	Treaty on the Functioning of the European Union
TURBINE	TrUsted Revocable Biometrics IdeNtitiEs
UNHCR	United Nations High Commissioner for Refugees
VIS	Visa information system
WCO	World Customs Organization
WP 29	Article 29 Data Protection Working Party
WPPJ	Working Party on Police and Justice

Annex D — List of Data Protection Officers

Situation as of 31 December 2014

ORGANISATION	NAME	E-MAIL
Council of the European Union	*Carmen LOPEZ RUIZ*	*Data.Protection@consilium.europa.eu*
European Parliament	*Secondo SABBIONI*	*Data-Protection@europarl.europa.eu*
European Commission	*Philippe RENAUDIERE*	*Data-Protection-officer@ec.europa.eu*
Court of Justice of the European Union	*Agostino Valerio PLACCO*	*Dataprotectionofficer@curia.europa.eu*
Court of Auditors	*Johan VAN DAMME*	*ECA-data-protection@eca.europa.eu*
European Economic and Social Committee (EESC)	*Lucas CAMARENA JANUZEC*	*data.protection@eesc.europa.eu*
Committee of the Regions (CoR)	*Rastislav SPÁC*	*data.protection@cor.europa.eu*
European Investment Bank (EIB)	*Alberto SOUTO DE MIRANDA (DPO)*	*dataprotectionofficer@eib.org*
European External Action Service (EEAS)	*Carine CLAEYS*	*data-protection@eeas.europa.eu*
European Ombudsman	*Rosita AGNEW*	*DPO-euro-ombudsman@ombudsman.europa.eu*
European Data Protection Supervisor (EDPS)	*Massimo ATTORESI (DPO)* *Elena JENARO TEJADA (Deputy DPO)*	*EDPS-DPO@edps.europa.eu*
European Central Bank (ECB)	*Frederik MALFRÈRE*	*DPO@ecb.europa.eu*
European Anti-Fraud Office (OLAF)	*Laraine LAUDATI*	*laraine.laudati@ec.europa.eu*
Translation Centre for the Bodies of the European Union (CdT)	*Martin GARNIER*	*data-protection@cdt.europa.eu*
Office for Harmonisation in the Internal Market (OHIM)	*Pedro DUARTE GUIMARÁES*	*DataProtectionOfficer@oami.europa.eu* *pedro.duarte@oami.europa.eu*
Agency for Fundamental Rights (FRA)	*Nikolaos FIKATAS*	*Nikolaos.Fikatas@fra.europa.eu*
Agency for the Cooperation of Energy Regulators (ACER)	*Paul MARTINET*	*Paul.Martinet@acer.europa.eu*
European Medicines Agency (EMEA)	*Alessandro SPINA*	*dataprotection@ema.europa.eu*
Community Plant Variety Office (CPVO)	*Gerhard SCHUON*	*schuon@cpvo.europa.eu*
European Training Foundation (ETF)	*Tiziana CICCARONE*	*Tiziana.Ciccarone@etf.europa.eu*
European Asylum Support Office (EASO)	*Paula Mello McCLURE (DPO)* *Francesca MARCON (Assistant DPO)*	*dpo@easo.europa.eu*

>>>

ORGANISATION	NAME	E-MAIL
European Network and Information Security Agency (ENISA)	*Konstantinos MOULINOS (DPO)* *Nikolaos CHRISTOFORATOS (Deputy DPO)*	*dataprotection@enisa.europa.eu*
European Foundation for the Improvement of Living and Working Conditions (Eurofound)	*Markus GRIMMEISEN*	*mgr@eurofound.europa.eu*
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	*Ignacio VÁZQUEZ MOLINÍ*	*Ignacio.Vazquez@emcdda.europa.eu*
European Food Safety Authority (EFSA)	*Claus REUNIS*	*dataprotectionofficer@efsa.europa.eu*
European Maritime Safety Agency (EMSA)	*Malgorzata NESTEROWICZ*	*malgorzata.nesterowicz@emsa.europa.eu*
European Centre for the Development of Vocational Training (Cedefop)	*Spyros ANTONIOU* *Jesus BUSTAMANTE*	*spyros.antoniou@cedefop.europa.eu* *jesus.bustamente@cedefop.europa.eu*
Education, Audiovisual and Culture Executive Agency (EACEA)	*Hubert MONET*	*hubert.monet@ec.europa.eu*
European Agency for Safety and Health at Work (EU-OSHA)	*Michaela SEIFERT*	*seifert@osha.europa.eu*
European Fisheries Control Agency (EFCA)	*Rieke ARNDT*	*efca-dpo@efca.europa.eu*
European Union Satellite Centre (EU SatCen)	*Jean-Baptiste TAUPIN*	*j.taupin@eusc.europa.eu*
European Institute for Gender Equality (EIGE)	*Ramunas LUNSKUS*	*Ramunas.Lunskus@eige.europa.eu*
European GNSS Supervisory Authority (GSA)	*Triinu VOLMER*	*Triinu.Volmer@gsa.europa.eu*
European Railway Agency (ERA)	*Zografia PYLORIDOU*	*dataprotectionofficer@era.europa.eu*
Consumers, Health and Food Executive Agency (Chafea)	*Despoina LEIVADINOU*	*chafea-data-protection@ec.europa.eu*
European Centre for Disease Prevention and Control (ECDC)	*Andrea AMMON (Acting)*	*dpo@ecdc.europa.eu*
European Environment Agency (EEA)	*Olivier CORNU*	*Olivier.Cornu@eea.europa.eu*
European Investment Fund (EIF)	*Jobst NEUSS*	*j.neuss@eif.org*
European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)	*Andrzej GRAS*	*Andrzej.gras@frontex.europa.eu*
European Securities and Markets Authority (ESMA)	*Sophie VUARLOT-DIGNAC (Acting DPO)* *Enrico GAGLIARDI (Deputy DPO)*	*sophie.vuarlot-dignac@esma.europa.eu*
European Aviation Safety Agency (EASA)	*Francesca PAVESI (DPO)* *Frank MANUHUTU (deputy DPO)*	*Francesca.Pavesi@easa.europa.eu*

>>>

ORGANISATION	NAME	E-MAIL
Executive Agency for Small and Medium-sized Enterprises (EASME)	*Elke RIVIERE (DPO)* *Ana Elen Pallarés ALLUEVA (Deputy DPO)*	*Elke.RIVIERE@ec.europa.eu*
Innovation and Networks Executive Agency (INEA)	*Zsófia SZILVÁSSY*	*inea-dpo@ec.europa.eu* *zsofia.szilvassy@ec.europa.eu*
European Banking Authority (EBA)	*Joseph MIFSUD*	*joseph.mifsud@eba.europa.eu*
European Chemicals Agency (ECHA)	*Bo BALDUYCK*	*bo.balduyck@echa.europa.eu*
European Research Council Executive Agency (ERCEA)	*Vanesa HERNANDEZ GUERRERO*	*Vanesa.Hernandez-Guerrero@ec.europa.eu*
Research Executive Agency (REA)	*Evangelos TSAVALOPOULOS*	*evangelos.tsavalopoulos@ec.europa.eu*
European Systemic Risk Board (ESRB)	*Frederik MALFRÈRE*	*DPO@ecb.europa.eu*
Fusion for Energy	*Angela BARDENHEWER-RATING*	*Angela.Bardenhewer-Rating@f4e.europa.eu*
SESAR Joint Undertaking	*Daniella PAVKOVIC*	*Daniella.Pavkovic@sesarju.eu*
ECSEL	*Anne SALAÜN*	*Anne.Salaun@ecsel.europa.eu*
Clean Sky Joint Undertaking	*Bruno MASTANTUONO*	*Bruno.Mastantuono@cleansky.eu*
Innovative Medicines Initiative Joint Undertaking	*Estefania RIBEIRO*	*Estefania.Ribeiro@imi.europa.eu*
Fuel Cells & Hydrogen Joint Undertaking	*Nicholas BRAHY*	*nicolas.brahy@fch.europa.eu*
European Insurance and Occupations Pensions Authority (EIOPA)	*Catherine COUCKE* *Natacha ROSEMARY (Deputy DPO)*	*catherine.coucke@eiopa.europa.eu* *Natacha.Rosemary@eiopa.europa.eu*
Collège européen de police (CEPOL)	*Leelo KILG-THORNLEY*	*leelo.kilg-thornley@cepol.europa.eu*
European Institute of Innovation and Technology (EIT)	*Beata GYORI-HARTWIG*	*eit-dpo@eit.europa.eu*
European Defence Agency (EDA)	*Gabriele BORLA*	*gabriele.borla@eda.europa.eu*
Body of European Regulators for Electronic Communications (BEREC)	*Michele Marco CHIODI*	*Michele-Marco.CHIODI@berec.europa.eu*
European Union Institute for Security Studies (EUISS)	*Nikolaos CHATZIMICHALAKIS*	*nikolaos.chatzimichalakis@iss.europa.eu*
eu-LISA	*Fernando DA SILVA*	*Fernando.pocas-da-silva@eulisa.europa.eu*

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

Prior Checks

Development programme for SG middle managers

Opinion of 14 January 2014 on a notification for prior checking regarding the "SG - Development programme for SG middle managers, use of self-perception questionnaire ("PERFORMANSE") and 360° tool of feedback on leadership competencies" (Case 2013-1290)

Staff evaluation, probationary reports and promotion - EIOPA

Opinion of 16 January 2014 on a notification for prior checking regarding the processing of personal data in the context of staff evaluation, probationary reports and promotion at the European Insurance and Occupational Pensions Authority (EIOPA) (Case 2013-0800)

Psychological or sexual harassment - EDA

Opinion of 21 January 2014 on a notification for prior checking regarding on the procedure following alleged psychological or sexual harassment, European Defence Agency (Case 2013-0874)

Update of Annual Evaluation / CDR – EC

Letter of 30 January 2014 to the EC DPO concerning the update of the annual evaluation / CDR due to new Staff Regulations relating to the further use of an unsatisfactory CDR for blocking advancement in step (Case 2013-1274)

DEVCO IT-tool (DEVIT)

Opinion of 30 January 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the DEVCO IT-tool (DEVIT) (Case 2013-1230)

SERMED Electronic Health Records - EC (DG HR)

Opinion of 30 January 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the use of SERMED for Electronic Heath Records (Case 2013-0146)

Leave and flexitime - EIT

Opinion of 3 February 2014 on the notification for prior checking from the Data Protection Officer of the European Institute of Innovation and Technology regarding leave and flexitime (Case 2013-0812)

Staff Selection and Appointment Procedures - EEAS

Opinion of 4 February 2014 on a notification for prior checking concerning Staff Selection and Appointment Procedures for Officials and Temporary Agents in the EEAS (Case 2013-0876)

Leave management - ENISA

Opinion of 5 February 2014 on the notification for prior checking from the Data Protection Officer of the European Network and Information Security Agency in the field of leave management (Case 2013-0594)

Participatory surveillance research project - JRC/IPSC

Opinion of 5 February 2014 on a notification for prior checking received from the Data Protection Officer of the European Commission related to the "Participatory surveillance research project with evacuation exercise at the JRC/IPSC institute" (Case 2012-0824)

Records of absence - ACER

Opinion of 6 February 2014 on the notification for prior checking from the Data Protection Officer of the Agency for the Cooperation of Energy Regulators concerning records of absence (sick leave and special leave), the establishment of annual leave entitlements, the recording of staff annual leave and part time work (Case 2013-0351)

Call for expressions of interest for contract staff in Nicosia/Cyprus - DG Enlargement

Opinion of 17 February 2014 on the notification for prior-checking concerning the processing of personal data in the context of the call for expressions of interest for contract staff in Nicosia/Cyprus within DG Enlargement (Case 2013-0672)

Risk analysis for fraud prevention and detection in the management of ESF and ERDF - EC

Opinion of 17 February 2014 on a notification for Prior Checking received from the Data Protection

Officer of the European Commission regarding the "Risk analysis for fraud prevention and detection in the management of ESF and ERDF" - ARACHNE (Case 2013-0340)

Staff Evaluation Procedures – GSA

Opinion of 19 February 2014 on the notifications for prior checking concerning staff evaluation, probation and reclassification (Case 2011-978, 2011-979, 2011-980)

Promotion Procedure – EEA

Opinion of 19 February 2014 on the notification for prior checking concerning promotion procedure at the European Environment Agency (Case 2013-865)

Public Procurement Procedure - REA

Opinion of 19 February 2014 on the notification for prior checking concerning public procurement procedure at the Research Executive Agency (Case 2013-271)

Accident and occupational disease procedure - ECB

Opinion of 20 February 2014 on the notification for prior checking received from the Data Protection Officer of the European Central Bank (ECB) concerning the "accident and occupational disease procedure" (Case 2012-0792)

Personnel selection and recruitment: update on introduction of e-recruitment tool - INEA (formerly TEN-T EA)

Opinion of 27 February 2014 on the notification for prior checking received from the Data Protection Officer of the Innovation and Networks Executive Agency (INEA - formerly TEN-T EA) concerning the introduction of an e-recruitment tool for personnel selection and recruitment (Case 2013-1067)

Early Warning System - ERCEA

Opinion of 3 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Research Council Executive Agency regarding the use of the Early Warning System (Case 2012-0823)

Teleworking - REA

Opinion of 3 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the Research Executive Agency regarding the processing of personal data concerning teleworking (Case 2013-0857)

Teleworking - ECHA

Opinion of 3 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Chemicals Agency regarding the use of teleworking (Case 2013-0566)

Pilot Project on Occasional Teleworking - ERCEA

Opinion of 3 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Research Council Executive Agency regarding a pilot project on the use of occasional teleworking (Case 2013-0552)

Teleworking - EACEA

Opinion of 3 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the Education, Audiovisual and Culture Executive Agency regarding the processing of personal data concerning teleworking (Case 2013-0794)

Teleworking - EFSA

Opinion of 3 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Food Safety Agency regarding the processing of personal data concerning teleworking (Case 2013-1378)

Public procurement - SESAR JU

Opinion of 17 March 2014 on the notification for prior checking received from the Data Protection Officer of the of the EU Joint Undertaking for Single European Sky Air Traffic Management Research (SESAR JU) concerning public procurement (Case 2011-0927)

Panel for Financial Irregularities - ECA

Opinion of 17 March 2014 on the notification for prior checking received from the Data Protection Officer of the European Court of Auditors concerning the ECA's Panel for Financial Irregularities (Case 2013-0846)

Staff recruitment at the European Institute of Innovation and Technology - EIT

Opinion of 17 March 2014 on the notification for prior checking concerning the processing of

personal data in the context of staff recruitment at the European Institute of Innovation and Technology (EIT) (Case 2013-0811)

Safety and Environmental Inspections - JRC

Opinion of 18 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the JRC regarding safety and environmental inspections at the KRC Petten site (Case 2012-0783)

Individual productivity and timeliness - OHIM

Opinion of 18 March 2014 on a notification for Prior Checking received from the Data Protection Officer of the OHIM regarding the "follow-up of individual productivity and timeliness" (Case 2013-0680)

Processing of Personal Data - ECJ

Opinion of 18 March 2014 on the notification for prior checking of the processing of personal data when appointing members of the Court of Justice, the General Court and the Civil Service Tribunal (Case 2014-0017)

Time management - INEA (formerly TEN-T EA)

Opinion of 19 March 2014 on the notification for prior checking from the Data Protection Officer of the Innovation and Networks Executive Agency concerning time management (Case 2013-0360)

Recording of working hours and flexitime administration - Cedefop

Opinion of 19 March 2014 on the notification for prior checking from the Data Protection Officer of the European Centre for the Development of Vocational Training concerning recording of working hours and flexitime administration (Case 2012-0679)

Passation de marchés publics et l'octroi de subventions - EP

Avis du 25 mars 2014 sur Notification de contrôle préalable concernant la passation de marchés publics et l'octroi de subventions au Parlement européen (Dossier 2013-0760)

Activity of the Mediation Service - EEAS

Opinion of 25 March 2014 on the notification for prior checking received from the Data Protection Officer (DPO) at the European External Action Service on the "activity of the mediation service" (Case 2013-0518)

Processing of health data - EIT

Opinion of 26 March 2014 on the notification for prior checking concerning the processing of health data at the European Institute of Innovation and Technology (EIT) (Case 2013-0814)

Processing of health data - BEREC

Opinion of 26 March 2014 on the notification for prior checking concerning the processing of health data at the Body of European Regulators for Electronic Communications ("BEREC") (Case 2013-0888)

Processing of health data in the workplace - CEPOL

Opinion of 26 March 2014 on the notification for prior checking concerning the processing of health data in the workplace (CEPOL) (Case 2013-0893)

Selection procedures for officials, temporary and contract agents and trainees - OHIM

Opinion of 26 March 2014 on the notification for prior checking concerning selection procedures for officials, temporary and contract agents and trainees at the Office for Harmonization in the Internal Market ("OHIM") (Case 2012-0852)

Selection procedures for temporary agents - EIGE

Opinion of 2 April 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of the European Institute for Gender Equality (EIGE) concerning EIGE's "selection procedures for temporary agents, contract agents, seconded national experts, trainees and interims" (EIGE) (Case 2013-0703)

Public procurement - EO

Opinion of 2 April 2014 on the notification for prior checking received from the Data Protection Officer of the European Ombudsman (EO) concerning public procurement (Case 2013-0875)

Self-assessment tool "PerformanSe" - EP

Opinion of 7 April 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of the European Parliament concerning the self-assessment tool "PerformanSe" (Case 2013-0772)

Personal data processing operations on leave - European Central Bank

Opinion of 8 April 2014 on the notification for prior checking received from the Data Protection Officer of the European Central Bank concerning the personal data processing operations on leave (Case 2013-0413)

Public procurement - F4E

Opinion of 15 April 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of the EU Joint Undertaking for Fusion for Energy (F4E) concerning public procurement and grants as well as selection and management of external experts (Case 2013-0759 & 1018)

Selection and management of experts - EASME

Opinion of 15 April 2014 on the notification for prior checking received from the Executive Agency for Small and Medium-sized Enterprises (EASME) on the selection and management of experts for evaluation activities in the field of Intelligence Energy Europe (IEE), Eco innovation (ECO-I) and Marco Polo programmes (Case 2013-0913)

Selection of the members for the Administrative Board of Review - ECB

Opinion of 23 April 2014 on the notification for prior checking received from the Data Protection Officer of the European Central Bank (ECB) concerning the selection of the members and alternates for the Administrative Board of Review (Single Supervisory Mechanism) (Case 2014-0394)

Processing of personal data with regard to the freezing of assets - Council

Opinion of 7 May 2014 on the notification for prior checking received from the Data Protection Officer of the Council of the European Union regarding the processing of personal data for restrictive measures with regard to the freezing of assets - Council (Case 2012-0724, 2012-0725, 2012-0726)

Dispositif de vérification biométrique - PE

Avis du 15 mai 2014 sur une notification de contrôle préalable reçue du délégué à la protection des données du Parlement européen concernant le dossier "Dispositif de vérification biométrique" (Dossier 2013-1110)

Fixation of individual rights - GSA

Opinion of 19 May 2014 on the notification received from the Data Protection Officer of the European Global Navigation Satellite Systems Agency (GSA) on the fixation of individual rights (Case 2014-0468)

Organisation of an internal competition - CoR

Opinion of 20 May 2014 on the notification received from the Committee of the Regions on the organisation of an internal competition under Article 29(3) of the Staff Regulations (Case 2013-0958)

Public procurement - EEAS

Opinion of 23 May 2014 on the notification for prior checking received from the Data Protection Officer of the European External Action Service concerning public procurement (Case 2013-0584)

Registration, selection and management of independent experts - REA

Opinion of 23 May 2014 on the notification for prior checking received from the Data Protection Officer of the Research Executive Agency concerning registration, selection and management of independent experts (Case 2013-0855)

Staff evaluation - ECA

Opinion of 23 May 2014 on the notification for prior checking received from the Data Protection Officer of the European Court of Auditors concerning staff evaluation - COMPASS2 (Case 2013-0907)

Staff evaluation and probation - Clean Sky

Opinion of 23 May 2014 on the notification for prior checking received from the Data Protection Officer of the Clean Sky Joint Undertaking concerning staff evaluation and probation (Case 2013-0915)

Anti-harassment procedures - EFCA

Opinion of 23 May 2014 on the notification for prior checking received from the Executive Director of the European Fisheries control Agency (EFCA) concerning anti-harassment procedures and the selection of confidential counsellors (Case 2014-0430)

Recruitment of interim agents - GSA

Opinion of 23 May 2014 on the notification for prior checking received from Executive Director of the

European Global Navigation Satellite Systems Agency (GSA) concerning selection and recruitment of interim agents (Case 2014-0475)

Processing of health data in the workplace - EIGE

Opinion of 23 May 2014 on the notification for prior checking received from the director of the European Institute for Gender Equality concerning processing of health data in the workplace (Case 2013-0721)

Development programme for middle managers - EC

Opinion of 23 May 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of DG COMP concerning the DG COMP Development programme for COMP middle managers (Case 2014-0446)

Public procurement - EU OSHA

Opinion of 23 May 2014 on the notification for prior checking received from the Data Protection Officer of the European Agency for Safety and Health at Work concerning public procurement (Case 2013-0734)

Internal recruitment - GSA

Opinion of 27 May 2014 on the notification for prior checking received from the Data Protection Officer of the European Global Navigation Satellite Systems Agency (GSA) concerning internal recruitment (Case 2012-0300)

Recruitment of temporary agents and contract agents - ACER

Opinion of 28 May 2014 on the notification for prior checking received from the Data Protection Officer of the Agency for the Cooperation of Energy Regulators (ACER) concerning the recruitment of temporary agents and contract agents (Case 2012-1012)

Selection of seconded national experts - ACER

Opinion of 28 May 2014 on the notification for prior checking received from the Data Protection Officer of the Agency for the Cooperation of Energy Regulators concerning the selection of seconded national experts (Case 2012-1013)

Gestion du Centre socio-culturel et sportif du SGC - Conseil

Avis du 4 Juin 2014 sur la notification d'un contrôle préalable reçue du Délégué à la protection des données du Secrétariat général du Conseil de l'Union européenne concernant la "Gestion du Centre socio-culturel et sportif du SGC" (Dossier 2012-0972)

Public procurement - ERA

Opinion of 12 June 2014 on the notification for prior checking received from the Data Protection Officer of the European Railway Agency concerning public procurement (Case 2013-0990)

Public procurement and selection of external experts - Chafea

Opinion of 12 June 2014 on the notification for prior checking received from the Data Protection Officer of the Consumers, Health and Food Executive Agency (Chafea) concerning public procurement and selection of external experts (Case 2013-1032+1033)

Public procurement - EASO

Opinion of 12 June 2014 on the notification for prior checking received from the Data Protection Officer of the European Asylum Support Office (EASO- concerning public procurement (Case 2013-1017)

Recrutement des fonctionnaires - CESE

Avis du 20 Juin 2014 concernant la notification du Comité économique et social européen concernant la procédure de sélection et de recrutement des fonctionnaires (Dossier 2013-0796)

Prevention of harassment - ECDC

Opinion of 23 June 2014 on the notification for prior checking received from the Director of the European Centre for Disease prevention and Control Agency (ECDC) concerning prevention of harassment and selection of confidential counsellors (Case 2014-0481)

Public procurement - ESMA

Opinion of 1 July 2014 on the notification for prior checking received from the Data Protection Officer of the European Securities and Markets Authority concerning public procurement (Case 2013-1165)

Public procurement, grant procedures and selection & use of external experts - IMI

Opinion of 1 July 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of the Innovative Medicines Initiative Joint Undertaking (IMI) concerning public procurement, grant procedures and selection and use of external experts at the Innovative Medicine Joint Undertaking (Case 2013-1162)

Public procurement - TEN-T EA

Opinion of 1 July 2014 on the notification for prior checking received from the Data Protection Officer at the Innovation and Networks Executive Agency concerning public procurement (Case 2013-1231)

Public procurement - BEREC

Opinion of 1 July 2014 on the notification for prior checking received from the Data Protection Officer at the Office of the Body of the European Regulators for Electronic Communications concerning public procurement (Case 2013-1175)

How to deal with information on scientific misconduct - ERCEA

Opinion of 9 July 2014 on the notification for prior checking received from the Data Protection Officer of the European Research Council Executive Agency concerning the procedure on how to deal with information on scientific misconduct (Case 2014-0538)

Internal Staff Transfers - EFSA

Opinion of 9 July 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of the European Food Safety Authority concerning transfer in the interest of the services within EFSA (Case 2013-1396)

Experts Selection and Management - ERCEA

Opinion of 9 July 2014 the notification for prior checking received from the Data Protection Officer of the European Research Council Executive Agency (ERCEA) concerning IDEAS - ERCEA of Experts Selection and Management (Case 2013-0575)

Public procurement - EMSA

Opinion of 17 July 2014 on the notification for prior checking received from the data protection officer (DPO) of the European Maritime Safety Agency (EMSA) concerning public procurement (Case 2013-1271)

Public procurement, selection and use of external experts - Clean Sky

Opinion of 17 July 2014 on the notification for prior checking received from the data protection officer (DPO) of the Clean Sky Joint Undertaking concerning public procurement, grant procedure as well as selection and use of external experts (Case 2013-1270)

Promotion, certification and attestation - EEAS

Opinion of 17 July 2014 on the notification for prior checking concerning promotion, certification and attestation of the EEAS officials (Case 2013-1034, 1035, 1036)

Appraisal, probation and management probation - EU-OSHA

Opinion of 17 July 2014 on the notification for prior checking received from the data protection officer (DPO) of the European Agency for Health and Safety at Work (EU-OSHA) concerning the appraisal, probation and management probation of the Director (Case 2014-0563)

Recruitment procedure for contract staff with a disability - European Parliament

Opinion of 17 July 2014 on the notification for prior checking received from the Director of DG Personnel at the European Parliament concerning the selection and recruitment procedure for contract staff with a disability (Case 2013-0608)

Recruitment of trainees with a disability - EP

Opinion of 17 July 2014 on the notification received from the European Parliament on the selection and recruitment of trainees with a disability within the Secretariat of the Parliament (Case 2013 0607)

Processing of health data - Cedefop

Opinion of 17 July 2014 on the notification for prior checking received from the Director of the European Centre for the Development of Vocational Training (Cedefop) concerning the processing of health data for medical part-time work (Case 2012-0384)

Special allowances - Court of Justice

Opinion of 17 July 2014 on the notification received from the Court of Justice of the European Union on special allowances (Case 2012-0611)

Assmal2 système de la gestion du régime commun d'assurance maladie des institutions de l'UE - Commission européenne (DG DIGIT)

Avis du 17 juillet 2014 concernant la notification de la Commission européenne concernant Assmal2 système de la gestion du régime commun d'assurance maladie des institutions de l'UE (Dossier 2013-0193)

Aménagement du temps de travail pour allaitement - Cour de justice

Avis du 17 juillet 2014 concernant la notification du Cour de justice concernant l'aménagement du temps de travail pour allaitement (Dossier 2013-0050)

Public procurement - ECB

Opinion of 17 July 2014 on the notification for prior checking received from the data protection officer (DPO) of the European Central Bank (ECB) concerning public procurement (Case 2013-1408)

Early Warning System (EWS) - REA

Opinion of 22 July 2014 on a notification for Prior Checking received from the Data Protection Officer of the Research Executive Agency regarding the processing operation on personal data concerning the "Early Warning System (EWS) at the Research Executive Agency" (Case 2012-0981)

Third Country Nationals accessing the Joint Research Centre sites

Opinion of 22 July 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Commission on the Security opinions on the Third Country Nationals accessing the Joint Research Centre sites (Case 2013-1020)

Public procurement and grant procedures - CEPOL

Opinion of 23 July 2014 on the notification received from the Data Protection Officer (DPO) of the European Police College (CEPOL) concerning public procurement and grant procedures (Case 2013-1394 & 1395)

Human resources needs analysis - OLAF

Opinion of 23 July 2014 on a notification for Prior Checking received from the Data Protection Officer of OLAF regarding their "human resource needs analysis" (Case 2014-0012)

Selection of EPIET and EUPHEM fellows - ECDC

Opinion of 25 July 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of ECDC on a set of processing operations named "selection of EPIET and EUPHEM fellows" (Case 2013-0780)

Administrative inquiries and disciplinary proceedings - EFCA

Opinion of 3 September 2014 on the notification for prior-checking on the processing operations related to selection and management of interim workers at the European Fisheries Control Agency (EFCA) (Case 2014-0628)

Selection and management of interim workers - EFSA

Opinion of 5 September 2014 on the notification for prior-checking on the processing operations related to selection and management of interim workers at the European Food Safety Authority (EFSA) (Case 2013-1059)

Recruitment of staff - EBA

Opinion of 16 September 2014 on prior checking notifications concerning the recruitment of temporary agents, contract agents and seconded national experts at the European Banking Authority (Case 2013-1066)

Activity of the network of the confidential counsellors - EEAS

Opinion of 16 September 2014 on prior checking notifications concerning activity of the network of the confidential counsellors and the selection of the confidential counsellors at the EEAS (Case 2013-0957)

Asylum Intervention Pool - EASO

Opinion of 18 September 2014 on a notification for Prior Checking received from the Data Protection Officer of the European Asylum Support Office (EASO) regarding the Asylum Intervention Pool (Case 2013-1228)

"SYSPER2 - Hardship" Time Management - EASO

Avis du 29 septembre 2014 sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission Européenne à propos du dossier " SYSPER2 - Hardship" (Case 2013-1276)

Traineeships - EFCA

Opinion of 9 October 2014 on notification for prior checking received from the Data Protection Officer of the European Fisheries Control Agency regarding traineeships (Case 2014-0637)

Breach Reporting Mechanism - European Central Bank

Opinion of 3 November 2014 on notification for prior checking received from the Data Protection Officer of the European Central Bank (ECB) regarding their Breach Reporting Mechanism (BRM) (Case 2014-0871)

Authorisation Division Procedures - European Central Bank

Opinion of 3 November 2014 on notification for prior checking received from the Data Protection Officer of the European Central Bank (ECB) regarding their Authorisation Division Procedures (Case 2014-0888)

Selection of interim agents - F4E

Opinion of 28 November 2014 on a notification for prior checking received from the Data Protection Officer of the European Joint Undertaking for ITER and the Development of Fusion for Energy (F4E) regarding the selection of interim agents (Case 2013-0707)

Staff evaluation procedures - REA

Opinion of 28 November 2014 on notifications for prior checking received from the Data Protection Officer of the Research Executive Agency (REA) regarding probation, management probation, evaluation, reclassification and evaluation of the third language working knowledge (Case 2012-0692, 0693, 0694, 0695, and 0696)

Staff evaluation procedures - ETF

Opinion of 28 November 2014 on notifications for prior checking received from the Data Protection Officer of the European Training Foundation (ETF) regarding promotion and renewal of contracts of employment (Case 2012-0853 and 0854)

Staff evaluation procedures - IMI

Opinion of 28 November 2014 on a notification for prior checking received from the Data Protection Officer of the Innovative Medicines Initiative Joint Undertaking (IMI) regarding annual appraisal, probation and reclassification of contract agents (Case 2013-0378)

Staff evaluation procedures - EIGE

Opinion of 28 November 2014 on a notification for prior checking received from the Data Protection Officer of the European Institute for Gender Equality (EIGE) regarding probation and performance appraisal (Case 2013-0722)

Performance assessment: Contract Agent and Temporary Agent Contracts - Eurofound

Opinion of 28 November 2014 on a notification for prior checking received from the Data Protection Officer of the European Foundation for the Improvement of Living and Working Conditions (Eurofound) regarding performance assessment in Contract Agent and Temporary Agent contracts (Case 2014-0846)

Grant procedures and selection of external experts - INEA

Opinion of 28 November 2014 on notifications for prior checking received from the Data Protection Officer of the Innovation and Network Executive Agency regarding grant procedures and the selection of external experts (Case 2014-0487 and 2014-0488)

Whistleblowing Procedure - EO

Opinion of 4 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Ombudsman (EO) regarding the European Ombudsman's Whistleblowing Procedure (Case 2014-0828)

Business objects reporting platform - ERCEA

Opinion of 10 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Research Council Executive Agency (ERCEA) regarding the "Business Objects reporting platform" for the purpose of Human Resources reporting (Case 2013-0467)

Development programme - Commission

Opinion of 12 December 2014 on a prior checking notification of Development programme for DG MARE "Middle Management Programme – 360° Feedback leadership Circle" (Case 2014-0906)

Gestion des permis de port d'arme pour les agents désignés du Bureau de Sécurité - Conseil

Avis du 16 décembre 2014 sur la notification d'un contrôle préalable reçue du Délégué à la protection des données du Secrétariat général du Conseil de l'Union européenne concernant la "Gestion des permis de port d'arme pour les agents désignés du Bureau de Sécurité" (Dossier 2012-0923)

Annual Internal Mobility Exercise at Headquarters - EEAS

Opinion of 17 December 2014 on a notification for prior checking received from the Data Protection Officer of the European External Action Service (EEAS) regarding the annual internal mobility exercise at the EEAS headquarters (Case 2013-0509)

Customs File Identification Database - OLAF

Opinion of 17 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) regarding the Customs File Identification Database (FIDE) (Case 2013-1003)

Staff Selection - SESAR (JU)

Opinion of 17 December 2014 on a notification for prior checking received from the Data Protection Officer of the SESAR (Single European Sky ATM Research) Joint Undertaking regarding the selection of staff (Case 2013-0718)

Covert Surveillance - Court of Justice

Opinion of 17 December 2014 on a notification for prior checking received from the Data Protection Officer of the Court of Justice regarding covert surveillance (Case 2014-0598)

Recruitment of temporary and contract staff - SESAR (JU)

Opinion of 17 December 2014 on a notification for prior checking received from the Data Protection Officer of the SESAR (Single European Sky ATM Research) Joint Undertaking regarding the recruitment of temporary and contract staff (Case 2013-0719)

Selection and Recruitment - REA

Opinion of 17 December 2014 on a notification for prior checking received from the Data Protection Officer of the Research Executive Agency (REA) regarding the selection and recruitment of contract and temporary agents, seconded Commission officials, interim staff, internal recruitment, and the administration of spontaneous applications (Case 2012-0057, 0058, 0059, 0060, 0061, 0063, 0065, 0066 and 0067)

Administrative inquiries and disciplinary proceedings - ERCEA, EACEA, INEA, Chafea, REA and EASME

Joint opinion of 18 December 2014 on a series of six notifications for prior checking received from the Data Protection Officers of the European Research Council Executive Agency (ERCEA), the Education, Audiovisual and Culture Executive Agency (EACEA), the Innovation and Networks Executive Agency (INEA formerly TEN-T EA), the Consumers, Health, Agriculture and Food Executive Agency (Chafea), the Research Executive Agency (REA) and the Executive Agency for Small and Medium-sized Enterprises (EASME formerly EACI) concerning Administrative inquiries and disciplinary proceedings (Case 2014-0805, 2014-0723, 2014-0136, 2013-1012, 2013-1022, 2014-0937)

Staff Performance Appraisal - Eurofound

Opinion of 18 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Foundation for the Improvement of Living and Working Conditions (Eurofound) concerning data processing related to Staff Performance Appraisal (Case 2014-0938)

Training - EU SatCen

Opinion of 18 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Union Satellite Centre (EU SatCen) concerning training (Case 2014-0599)

Access to Documents - EU SatCen

Opinion of 18 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Union Satellite Centre (EU

SatCen) concerning requests for access to documents (Case 2014-0600)

Pension Rights - EU SatCen

Opinion of 18 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Union Satellite Centre (EU SatCen) concerning the management of pension rights (Case 2014-0604)

Access to office and badges - EU SatCen

Opinion of 18 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Union Satellite Centre (EU SatCen) concerning the access to office and badges (Case 2014-0613)

Anti-harassment policy - EIGE

Opinion of 18 December 2014 on a notification for prior checking received from the Data Protection Officer of the European Institute for Gender Equality (EIGE) concerning the anti-harassment policy (Case 2013-0732)

Recruitment - BEREC

Opinion of 19 December on a notification for prior checking received from the Data Protection Officer of the Body of European Regulators of Electronic Communications (BEREC) Office regarding the recruitment of temporary agents, contract agents and seconded national experts (Case 2013-0841)

Non-prior Checks

Field Experiments carried out by Institute for Health and Consumer Protection - JRC

Letter of 9 January 2014 regarding prior checking notification of the collection and processing of data in the context field experiments undertaken by the Institute for Health and Consumer Protection of the Joint Research Centre (JRC) (Case 2013-1229)

Conflict of interest - Clean Sky

Letter of 29 January 2014 regarding prior checking notification of the collection and processing of data in the context of conflict of interest framework in place at the Clean Sky Joint Undertaking and the declarations of interest to be filled in by Joint Undertaking staff and other Joint Undertaking actors upon start of their assignment at Clean Sky (Case 2013-1269)

Traitement de données personnelles "Agenda" - Cour de Justice

Avis du 3 février 2014 sur la notification de contrôle préalable reçue du délégué à la protection des données (DPD) de la Cour de justice de l'Union européenne à propos du traitement de données personnelles "Agenda" (Dossier 2013-0712)

Safety and Environmental Investigations - JRC Petten

Letter of 18 March 2014 on the notification for prior checking of the processing operation concerning the Safety and Environmental Investigations at JRC Petten (Case 2012-0783)

Processing of personal data - INEA

Letter of 18 March 2014 concerning notification for prior-checking relating to the processing of personal data in the context of the management of personal files by the Innovation and Networks Executive Agency (INEA) (Case 2013-1365)

Access Control System (Iris Scan Technology) - Frontex

Letter of 24 March 2014 on the notification for prior checking from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union concerning the use of an access control system using Iris Scan Technology (Case 2010-1008)

Safety at work - JRC

Letter of 25 March 2014 regarding the processing operations concerning the Integrated Management System for safety at work within JRC Ispra (Case 2013-0162)

Evaluations by external contractors - ETF

Letter of 31 March 2014 concerning evaluations of effectiveness of the European Training Foundation (ETF) (Case 2012-0855)

Redress procedure in grants - ERCEA

Letter of 31 March 2014 concerning redress procedure in grants by the European Research Council Executive Agency (ERCEA) (Case 2012-0865)

Staff Regulations - EMSA

Letter of 06 May 2014 concerning the appeal procedure under Article 90 of the Staff Regulations in European Maritime Safety Agency (EMSA) (Case 2014-0261)

HR Software EU HR Allegro - GSA

Letter of 12 May 2014 on the notification for prior checking received from the Executive Director of the European GNSS Agency concerning the management of personnel files using the Human Resources software EU HR Allegro (GSA) (Case 2014-0474)

Fixation of individual rights - GSA

Letter of 19 May 2014 on the notification for prior checking received from the Executive Director of the European GNSS Agency concerning "fixation of individual rights" (GSA) (Case 2014-0468)

Enfant handicapé ou Maladie de longue durée - CoR

Lettre du 3 juin 2014 concernant la notification du Comité des régions relative à l'octroi de l'allocation pour enfant à charge doublée en cas d'un handicap ou d'une maladie de longue durée (Dossier 2014-0424)

Employment termination of the statutory staff - INEA

Letter of 3 June 2014 on the notification for prior checking received from the Data Protection Officer (DPO) of the Innovation and Networks Executive Agency (INEA) on the processing operations related to employment termination of the statutory staff (Case 2013-1309)

Hostile Environment Awareness Training (HEAT) - EEAS

Letter of 11 June 2014 concerning the processing operations related to Hostile Environment Awareness Training (HEAT) in the European External Action Service (EEAS) (Case 2014-0447)

Renewal of contracts for temporary and contract agents - INEA

Letter of 12 June 2014 concerning the processing operations related to renewal of contracts for temporary and contract agents in the Innovation and Networks Executive Agency (Case 2013-1288)

Management of the administrative and financial files of interinstitutional crèches and childcare facilities - OIB

Opinion of 1 July 2014 on the notification for prior checking concerning the processing operation "Management of the administrative and financial files of interinstitutional (after-school and outdoor) crèches and childcare facilities by the OIB" (Case 2012-0419)

Contract management - ECHA

Letter of 14 July 2014 concerning the processing operations related to contract management in the European Chemicals Agency (ECHA) (Case 2014-0625)

Management of incident or technical fault reports - EP

Letter of 24 July 2014 on the notification for prior-checking concerning "Management of incident or technical fault reports" within the European Parliament (Case 2014-0643)

Flexi-time Rules - EBA

Letter of 13 October July 2014 on the notification for prior-checking concerning the management of Flexi-time by the European Banking Authority (Case 2014-0496)

Evaluation of Outside Activities by Members of the ECA - ECA

Letter of 9 December 2014 on the notification for prior-checking concerning the evaluation of outside activities exercised by Members the European Court of Auditors (ECA) (Case 2012-0822)

Annual Declaration of Interests - EASA

Letter of 9 December 2014 on the notification for prior-checking concerning the annual declaration of interest by the members of the European Aviation Safety Agency (EASA) (Case 2012-0901)

Conflicts of Interest - IMI

Letter of 9 December 2014 on the notification for prior-checking concerning the management of conflicts of interest of Executive Director and Staff of the Innovative Medicines Initiative (IMI) (Case 2013-0723)

Application of Ethics and Conflicts of Interest Rules - EBA

Letter of 9 December 2014 on the notification for prior-checking concerning the application of Ethics and Conflicts of Interest Rules for the European Banking Authority (EBA) (Case 2013-1063)

Application of Ethics and Conflicts of Interest Rules - EIOPA

Joint Letter of 9 December 2014 on the notification for prior-checking concerning the application of Ethics and Conflicts of Interest Rules for the Executive Director and Staff of the Innovative Medicines Initiative (IMI) (Case 2013-0758, 2013-1416)

Avoiding Conflicts of Interest - EASO

Letter of 9 December 2014 on the notification for prior-checking concerning the avoidance of Conflicts of Interest for the European Asylum Support Office (EASO) (Case 2014-0556)

Application of Ethics and Conflicts of Interest Rules - ESMA

Letter of 9 December 2014 on the notification for prior-checking concerning the application of Ethics and Conflicts of Interest Rules for the European Securities and Markets Authority (ESMA) (Case 2013-0930)

Autorisations (activité extérieure, rémunération extérieure, mandat extérieure, etc.) - Cour de justice

Lettre du 9 décembre 2014 sur la notification pour contrôle préalable des autorisations (activités extérieures, rémunération extérieure, mandat extérieure, etc.) de la Cour de justice (Case 2013-0788)

Administrative Appeals - EASME (formerly EACI)

Letter of 18 December 2014 on the notification for prior-checking concerning Administrative appeals received from the Data Protection Officer of the European Agency for Small and Medium-sized Enterprises (EASME formerly known as EACI) (Case 2013-0837)

E-Learning Platform - EASO

Letter of 18 December 2014 on the notification for prior-checking concerning the use of an E-learning platform by the Data Protection Officer of the European Asylum Support Office (EASO) (Case 2014-0933)

Training and Expert Pool - EASO

Letter of 18 December 2014 on the notification for prior-checking concerning the processing of personal data in the management of a Training and Expert Pool by the Data Protection Officer of the European Asylum Support Office (EASO) (Case 2014-0935)

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

Opinions

In 2014 the EDPS issued Opinions on the following subjects (date of publication in brackets):

- Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking (17/02/14)
- Communication from the Commission to the Council and the European Parliament on 'Rebuilding trust in EU - US data flows' (19/2/2014)
- Eurojust/EPPO Regulations (5/03/2014)
- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member stateMember states and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (11/03/2014)
- The proposal for a directive on trade secrets (12/03/2014)
- EU-China Customs Agreement (14/03/2014)
- EDPS Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data (26/03/2014)
- Commission Proposal for a Regulation on a European network of Employment Services workers' access to mobility services and the further integration of labour markets (3/04/2014)
- The future development of the area of freedom, security and justice (4/06/2014)
- Commission Communication on Internet Policy and Governance (23/06/2014)
- Regulations on financial markets (11/07/2014)
- Commission Proposal for a Directive of the European Parliament and of the Council on single-member private limited liability companies (23/07/2014)
- Commission Decision on the protection of personal data in the European e-Justice Portal (5/09/14)
- Shareholders rights proposal (28/10/14)
- Communication from the Commission to the European Parliament and the Council on 'A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner' (26/11/14).

Formal comments

In 2014 the EDPS issued formal comments on the following subjects (date of publication in brackets):

- (17/01/2014) Regulations governing social security co-ordination (Cross border social security fraud)
- (12/02/2014) Data Protection and supervision of Europol
- (14/02/2014) Progress on the data protection reform package
- (20/02/2014) Proposal for a Regulation on official controls and other official activities performed to ensure the application of food and feed law, rules on animal health and welfare, plant health, plant reproductive material, plant protection products
- (12/03/2014) Public consultation on EU wide real-time traffic information
- (17/04/14) ICANN's public consultation on 2013 RAA Data Retention Specification, Data Elements and Legitimate Purposes for Collection and Retention
- (17/04/14) European Terrorist Finance Tracking System (TFTS) Communication
- (30/04/14) General Report on the activities of the European Union
- (11/07/2014) Proposal for a Directive of the European Parliament and of the Council on the dissemination of Earth observation satellite data for commercial purposes.
- (23/07/2014) Proposal for a Decision of the European Parliament and of the Council on establishing a European Platform to enhance cooperation in the prevention and deterrence of undeclared work

- (30/09/2014) Open consultation on the Commission Impact Assessment Guideline
- (3/10/2014) Proposal on cross-border enforcement of road safety traffic offences
- (3/12/2014) Proposal for a Regulation of the European Parliament and of the Council amending Regulation No 966/2012 on the financial rules applicable to the general budget of the Union.

Annex G — Speeches by the Supervisor and Assistant Supervisor in 2014

The Supervisor and the Assistant Supervisor continued to invest substantial time and effort in 2014 to explain their mission and to raise awareness of data protection in general.

On 4 December 2014, Giovanni Buttarelli and Wojciech Wiewiórowski took up their posts as EDPS and Assistant EDPS respectively. All speeches prior to this date refer to Peter Hustinx, EDPS and Giovanni Buttarelli, assistant EDPS.

European Parliament

22 January	Supervisor, Lunch debate on e-Call Regulation (Brussels)
31 March	Supervisor and Assistant Supervisor, LIBE Committee on EDPS Annual Report 2013 (Brussels)

Council

21 January	Supervisor, Polish Permanent Representation on Data Protection Day (Brussels)
12 February	Supervisor, Council WP on Europol Regulation (Brussels) (*)
13 March	Supervisor, Council WP on Eurojust Regulation (Brussels)

European Commission

1 April	Supervisor, European Consumer Summit (Brussels) (*)
20 June	Supervisor, Erasmus for Public Administration (Brussels)

Other EU institutions and bodies

20 January	Supervisor and Assistant Supervisor, 10 years EDPS (Brussels)
12 February	Supervisor, LEWP Conference on the Data Protection Supervision of Europol (Brussels)
7 April	Supervisor, ERA Conference on European Data Protection Law (Brussels) (*)
9 April	Supervisor, EESC Conference on citizens' rights in data protection (Brussels)
20 May	Supervisor, Ombudsman Conference on Draft Model Rules for Administrative Procedures (Brussels)
2 June	Supervisor and Assistant Supervisor, EDPS Workshop Privacy, Consumers, Competition and Big Data (Brussels)
26 September	Supervisor, Workshop on Internet Privacy Engineering (Brussels)
5 November	Supervisor, BFDI-EDPS Panel discussion on EU Data Protection Reform (Brussels)

International Conferences

24 January	Supervisor and Assistant Supervisor, Conference on Computers, Privacy and Data Protection (Brussels)
21 March	Supervisor, OECD Expert Roundtable on Privacy and Big Data (Paris)
5 May	Supervisor, OECD Annual Forum (Paris)
13 May	Supervisor, European Data Protection Day (Berlin)
14 May	Supervisor, UN Commission for Crime Prevention and Criminal Justice (Vienna)
21 May	Assistant Supervisor, INET 2014 (Istanbul) (*)
1 July	Supervisor, Privacy Laws and Business Annual Conference (Cambridge)
15 October	Supervisor, International Data Protection Conference (Mauritius) (*)

Other events

13 January	Supervisor, ZEI Fourth Bonn Conference on data protection, net neutrality and economic freedom' (Bonn) (*)

28 January	Supervisor, CEPS on Data Protection and Mass Surveillance (Brussels)
4 February	Supervisor, Inauguration of Federal Commissioner for Data Protection and Freedom of Information (Bonn) (*)
20 February	Supervisor, Insight Innovation Exchange (IIE) Conference (Amsterdam)
20 March	Supervisor, CIPL Workshop on Privacy Risks Assessment (Paris)
27 March	Supervisor, European Voice Roundtable on the Future of Data (Brussels)
1 April	Supervisor, European Consumer Summit 2014 Conference on Digital era (Brussels)
2 April	Supervisor, House of Lords EU Committee on EU-US Data Flows (London)
11 April	Supervisor, American Chamber of Commerce Digital Economy Committee on Privacy, Big Data and Competition (Brussels)
30 April	Supervisor, European Banking Federation on Financial Regulation and Data Protection (Brussels)
30 April	Supervisor, Telecom Italia & ETNO Workshop on a New Digital Agenda for Europe (Brussels)
8 May	Supervisor, Dutch Privacy Law Association on EU Data Protection Reform (Utrecht)
15 May	Supervisor, SECILE Workshop on Privacy and Counter-Terrorism (Durham)
19 May	Supervisor, HUB Lecture on EU Data Protection Reform (Brussels)
21 May	Assistant Supervisor, Inet 2014 Conference on Internet: Privacy and Digital Content, (Istanbul)
17 June	Supervisor, EReg - EUCARIS Annual Conference (Helsinki)
2 September	Supervisor, Economic Forum (Krynica)
12 September	Supervisor, Consensus Conference on Management of Conflicts of Interest (Köln)
20 September	Supervisor, UIA Seminar on Data Protection (Luxembourg)
31 October	Supervisor, ERA Conference on EU Data Protection and the Role of Courts (Paris)
4 November	Supervisor, CEIS Workshop on Digital Economy (Brussels)
4 November	Supervisor, Montgomery Club on Digital Privacy (Brussels)
13 November	Supervisor, Joint Conference of SurPRISE, PRISMS and PACT Research Projects (Vienna)
17 November	Supervisor, 80th Anniversary of Professor Spiros Simitis (Frankfurt)
18 November	Supervisor, CIPL Workshop on Privacy Risk Assessment (Brussels)
19 November	Supervisor, ECTA Regulatory Conference on EU Data Protection Reform (Brussels)
20 November	Supervisor, Dutch Electronic Commerce Platform on EU Data Protection Reform (The Hague)
27 November	Supervisor, Federal Conference Compliance Management on EU Data Protection Reform (Berlin)
28 November	Supervisor, EuroCommerce General Assembly on EU Data Protection Reform (Brussels)
12 December	Assistant Supervisor, PHAEDRA European and international cooperation in enforcing privacy: expectations and solutions for a reinforced cooperation (Krakow)

(*) Text available on the EDPS website

Annex H — Composition of EDPS Secretariat

Director, Head of Secretariat

Christopher DOCKSEY

Daniela OTTAVI
Planning/Internal Control Coordinator

Supervision and Enforcement

Sophie LOUVEAUX *Head of Unit*	Maria Verónica PEREZ ASINARI *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*
Daniela GUADAGNO* *Legal Officer/ Seconded National Expert*	Mario GUGLIELMETTI *Legal Officer*
Xanthi KAPSOSIDERI *Legal Officer*	Owe LANGFELDT *Legal Officer*
Anna LARSSON STATTIN *Legal Officer/ Seconded National Expert*	Antje PRISKER *Legal Officer*
Dario ROSSI* *Supervision and Enforcement Assistant* *Accounting Correspondent* *Financial ex post facto verifier*	Bénédicte RAEVENS *Legal Officer*
Snezana SRDIC *Legal Officer*	Tereza STRUNCOVA *Legal Officer*
Michaël VANFLETEREN* *Legal Officer*	Gabriela ZANFIR *Legal Officer*

Policy and Consultation

Hielke HIJMANS *Head of Unit (until 30/06/2014)*	Anne-Christine LACOSTE *Head of Unit a.i.*
Anna BUCHTA *Head of Litigation and Institutional Policy*	Isabelle CHATELIER *Head of Legislative Policy*
Alba BOSCH MOLINE *Head of international Cooperation*	Zsuzsanna BELENYESSY *Legal Officer*
Gabriel Cristian BLAJ *Legal Officer*	Christian D'CUNHA *Legal Officer*
Priscilla DE LOCHT* *Legal Officer*	Elena JENARO *Legal Officer* *Assistant Data Protection Officer (from 16/10/2014)*
Amanda JOYCE *Policy and Consultation Assistant*	Elise LATIFY* *Legal Officer*
Per JOHANSSON* *Legal Officer*	Jacob KORNBECK *Legal Officer*
Fabio POLVERINO *Legal Officer*	Vera POZZATO* *Legal Officer*

* Staff members who left the EDPS in the course of 2014

IT Policy

Achim KLABUNDE *Head of sector*	Luisa PALLA *Head of Records Management*
Erin ANZELMO* *Technology and Security Assistant*	Massimo ATTORESI *Technology and Security Officer* *Data Protection Officer (from 16/10/2014)*
Andy GOLDSTEIN *Technology and Security Officer* *LISO*	Malgorzata LAKSANDER *Technology and Security Officer*
Fidel SANTIAGO *Technology and Security Officer* *Deputy-LISO*	

Records management Group

Marta CORDOBA-HERNANDEZ *Administrative Assistant*	*Milena KEMILEVA** *Administrative Assistant*
Kim Thien LÊ *Administrative Assistant*	Séverine NUYTEN *Administrative Assistant*
Carolina POZO LOPEZ *Administrative Assistant*	Maria Jose SALAS MORENO *Administrative Assistant*

Information and Communication

Olivier ROSSIGNOL *Head of Sector*	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 a.i.* *Data Protection Officer (until 15/10/2014)*
Maria SANCHEZ LOPEZ *Head of Finance*	Pascale BEECKMANS *Finance Assistant* *GEMI*
Laetitia BOUAZZA-ALVAREZ *Administration Assistant*	Andrei Radu GHERMAN* *Human Resources Officer*
Anne LEVECQUE* *Human Resources Assistant* *Official Managing Leave*	Vittorio MASTROJENI *Human Resources Officer*
Julia MOLERO MALDONADO *Finance Assistant*	Aida PASCU* *Administration Assistant* *LSO*
Anne-Françoise REYNDERS *Human Resources Officer* *L&D Coordinator*	

* Staff members who left the EDPS in the course of 2014

QT-AA-15-001-EN-N

www.edps.europa.eu

@EU_EDPS

Publications Office

ISBN 978-92-9242-065-9

EDPS

European Data Protection Supervisor