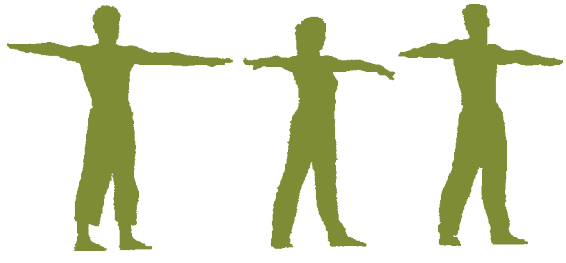
ISSN 1830-5482

Annual Report 2013

European Data Protection Supervisor

Annual Report

2013



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, 2014

ISBN 978-92-95076-87-7
doi: 10.2804/59280

Printed in Belgium

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

Contents

7 ADMINISTRATION, BUDGET AND STAFF

8 EDPS DATA PROTECTION OFFICER

9 MAIN OBJECTIVES FOR 2014

USER GUIDE

Following this guide, there is a mission statement and foreword to the 2013 Annual Report by Peter Hustinx, European Data Protection Supervisor and Giovanni Buttarelli, Assistant Supervisor.

Chapter 1 — **2013 Highlights** presents the main features of our work in 2013 and our achievements against key performance indicators in the various fields of activities.

Chapter 2 — **Supervision** describes the work done to monitor and ensure the compliance of EU institutions and bodies with their data protection obligations. This chapter presents an analysis of the main issues in prior checks, further work in the field of complaints, monitoring compliance and advice on administrative measures dealt with in 2013. It also includes information on data protection guidance delivered by the EDPS, either in thematic guidelines or in the context of training and workshops.

Chapter 3 — **Consultation** deals with developments in our advisory role, focusing on Opinions and comments issued on legislative proposals and related documents, as well as their impact in a growing number of areas. It contains an analysis of horizontal themes: new developments in policy and legislation and the on-going review of the EU data protection legal framework. The chapter also outlines the involvement of the EDPS in cases before the Court of Justice of the EU.

Chapter 4 — **Cooperation** describes our work in key forums such as the Article 29 Data Protection Working Party and the various groups ensuring coordinated supervision (by EDPS and national data protection authorities) of large scale IT-systems, as well as the European and international data protection conferences. It also covers our cooperation with international organisations and third countries

Chapter 5 — **Monitoring technology** gives a broad overview of technological trends that will have a likely impact on privacy and protection of personal data in the near future.

Chapter 6 — **Communication** presents our information and communication activities and achievements, including communication with the media, awareness-raising events, public information and online information tools.

Chapter 7 — **Administration, budget and staff** details the key areas within the EDPS organisation including budget issues, human resource matters and administrative agreements.

Chapter 8 — **EDPS Data Protection Officer** includes an update of the EDPS' register of processing operations in 2013.

Chapter 9 — **Main objectives for 2013** outlines our main priorities for 2014.

This Report concludes with a number of **annexes**. They include an overview of the relevant legal framework, provisions of Regulation (EC) No 45/2001, the list of Data Protection Officers, the lists of EDPS prior check Opinions and consultative Opinions, speeches given by the Supervisor and Assistant Supervisor and the composition of the EDPS secretariat.

An Executive Summary of this report which gives an overview of key developments in EDPS activities in 2013 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

MISSION STATEMENT, VALUES AND PRINCIPLES

The European Data Protection Supervisor is the European Union's independent data protection authority established under Regulation (EC) No. 45/2001 (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

We are pleased to submit the Annual Report on the activities of the European Data Protection Supervisor (EDPS) to the European Parliament, the Council and the European Commission, in accordance with Regulation (EC) No. 45/2001 and Article 16 of the Treaty on the Functioning of the European Union.

This report covers 2013 as the tenth year of activity of the EDPS as an independent supervisory authority, tasked with ensuring 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. It also covers the final year of our shared mandate as members of this authority.

Our Strategy 2013-2014, together with our Rules of Procedure and Annual Management Plan, have been sources of valuable guidance, articulating the vision and the methodology required to improve our capacity to work effectively in a climate of austerity. Our institution has now reached full maturity, with clear objectives and performance indicators.

Over the course of 2013, we paid particular attention to the different areas of activity implementing the action plan laid down in our Strategy. In the supervision of EU institutions and bodies, when processing personal data, we interacted with more data protection officers in more institutions and bodies than ever before. In addition, we have completed a number of surveys showing that most EU institutions and bodies, including many agencies, have made good progress in complying with the Data Protection Regulation, although there are still some which should increase their efforts.

In the consultation area, advising on new legislative measures, the review of the EU legal framework for data protection continued to be at the top of our agenda. The Digital Agenda and the privacy risks of new technologies were also significant features of 2013. However, the implementation of the Stockholm programme in the area of freedom, security and justice and issues in the internal market, such as financial sector reform, and in public health and consumer affairs, also had an impact on data protection. We also increased our cooperation with other supervisory authorities, particularly with regard to large-scale IT systems.

We wish to take this opportunity to thank those in the European Parliament, the Council and the Commission who supported our work and many others in different institutions and bodies who are responsible for the way in which data protection is delivered in practice. We would also like to encourage those who are dealing with important challenges ahead in this field.

Finally, we wish to express special thanks to our members of staff. Their level of quality is outstanding and this contributed greatly to our effectiveness during the entire mandate.

Peter Hustinx
European Data Protection Supervisor

Giovanni Buttarelli
Assistant Supervisor

1 2013 HIGHLIGHTS

1.1. General overview of 2013

Ten years after its foundation, the EDPS is a mature organisation, able to address the many challenges of a data protection authority in a highly dynamic environment. Our main operational challenge in 2013 was that our activities continued to grow both in scale and scope while the budget restraints and resource measures due to the financial crisis were still in place.

Our Strategy 2013-2014, together with our Rules of Procedure and Annual Management Plan have been sources of valuable guidance, articulating the vision and the methodology required to improve our capacity to work effectively and efficiently in a climate of austerity.

The legal framework[2] within which the EDPS acts provides for a number of tasks and powers which distinguish our three main roles of supervision, consultation and cooperation. These roles continue to serve as strategic platforms for our activities and are reflected in our mission statement:

- a supervisory role to monitor and ensure that EU institutions and bodies[3] comply with existing legal safeguards whenever they process personal information;
- a consultative role to advise EU institutions and bodies on all relevant matters, especially on proposals for legislation that have an impact on the protection of personal information;
- a cooperative role to work with national supervisory authorities and other relevant supervisory bodies, with a view to improving consistency in the protection of personal information.

These roles are examined in chapters 2, 3 and 4, where we present our vision, our main activities and the progress made in 2013. However, some of the key elements are summarised in this section.

In 2013 we improved our technological capabilities. Chapter 5 details the observations of selected technological developments that have particular relevance for privacy and data protection.

The importance of information and communication in our core activities also continues to grow and our communication work in 2013 is covered in Chapter 6.

All of our activities rely on effective management of financial, human and other resources and these are outlined in Chapter 7.

[2] See overview of legal framework in Annex A and extract from Regulation (EC) No 45/2001 in Annex B.

[3] The terms 'institutions' and 'bodies' of Regulation (EC) No 45/2001 are used throughout the report. This also includes EU agencies. For a full list, visit the following link: http://europa.eu/about-eu/institutions-bodies/index_en.htm

Supervision and enforcement

We saw an increase in the number of prior check notifications received in the context of our Supervision and Enforcement work. This increase is due primarily to the June 2013 deadline for *ex-post* prior check notifications for processing operations already in place. Despite the fact that for these *ex-post* cases, the EDPS is not bound by the two month deadline within which to adopt an Opinion, we have nevertheless strived to deliver our Opinion within a short timeframe. The increase in the number of Opinions we issued during the year is also a result of the high number of notifications received. We continued to follow up recommendations made in EDPS prior check Opinions already issued and were able to close a considerable number of cases.

The number of complaints we received decreased, partly due to better information and awareness of EDPS competencies, but also because of the effectiveness of our complaint submission form.

One of the features of the action plan as laid down in our Strategy 2013-2014 is to promote a 'data protection culture' within the EU institutions and bodies so that they are aware of their obligations and are accountable for complying with data protection requirements.

In light of this we continued to provide guidance and training to controllers, data protection officers (DPOs) and data protection coordinators (DPCs) primarily in the form of Guidelines on Public Procurement, Grants and External Experts; basic training for new DPOs on the prior checking procedure; special training for the DPOs of five EU Joint Undertakings. Our awareness raising initiatives within EU institutions and bodies included the organising of workshops for controllers at the European Training Foundation (ETF) and the European Defence Agency (EDA) and general workshops in the field of e-Communication, the use of mobile devices in the workplace and on websites managed by EU institutions and bodies.

An important element of our work also focused on raising awareness of data protection at all levels of management, in particular by visiting institutions or bodies when there has been a lack of compliance with the data protection rules or a lack of communication. A visit generally comprises an on-site visit by the EDPS or Assistant EDPS and usually produces good results in terms of engaging management and raising awareness of data protection.

Also key was our on-going dialogue with controllers, DPOs and DPCs to support the work of DPOs. These meetings help us gain a better understanding of the constraints of institutions in order to offer practical advice. Many meetings were held with controllers either in the course of prior check work or in the follow up to Opinions and decisions. The DPO network meetings, bilateral meetings and the helpline for DPOs were useful channels of communication for our work with the DPOs and DPCs.

The results of our fourth general stock taking exercise, Survey 2013, which was launched on 17 June 2013 as part of our compliance monitoring activities, will be published in early 2014. We also published a report compiling the results of the survey on the status of the DPCs at the European Commission in January 2013.

We adopted our Inspection Policy in 2013 which sets out the main elements of the EDPS inspection procedure, offers guidance to all those concerned and ensures transparency to stakeholders. A comprehensive internal inspection manual offering guidance to EDPS colleagues dealing with inspections, compiled on the basis of experience in previous inspections, was also adopted.

Consultation

In recent years, the number of EDPS Opinions issued for proposals on EU legislation and related documents have increased steadily. In 2013 this number decreased: we issued 20 legislative Opinions and 13 sets of formal comments, and we provided informal advice to the Commission or other institutions in 33 cases. The two main reasons for this decrease are that our efforts to focus on strategic priorities were successful and also that many resources were dedicated to the reform of the data protection framework.

Throughout 2013, we continued to be closely involved in the on-going work on the reform of the EU data protection framework. On 15 March 2013, we sent additional comments on the reform to the European Parliament, the Commission and the Council. We also continued our involvement in the discussions that followed in both Parliament and Council.

In addition to this, the Commission published a large number of legislative proposals affecting the fundamental right to the protection of personal data.

We addressed the issue of the Digital Agenda and internet several times, for example, in our Opinion on the commission communication on the Digital Agenda for Europe – Driving European growth digitally, our Opinion on the European Single Market for electronic communications and the Opinion on a green paper entitled Preparing for a fully converged audio-visual world: Growth, Creation and Values.

In the Area of Freedom, Security and Justice (AFSJ), we published Opinions on Europol, the EU cyber security strategy and smart borders as well as on EU-Canada passenger name records (PNR) and the European information exchange model.

Opinions of particular note relating to the internal market were our Opinions on anti-money laundering and terrorist financing, payments in the internal market, European company law and corporate governance and electronic invoicing in public procurement.

In the area of eHealth we would highlight our Opinions on medical devices, drug precursors and the eHealth action plan.

Court cases

In 2013, the EDPS intervened in a number of cases before the Court of Justice of the European Union and the Civil Service Tribunal.

The EDPS made oral submissions at a hearing before the Grand Chamber of the Court of Justice in a preliminary reference procedure. This hearing concerned joined cases Digital Rights Ireland (C-293/12) and Seitlinger and Others (C-293/12). Both cases relate to the validity of the Data Retention Directive 2006/24/EC.

It was the first time that the Court had invited the EDPS to appear at a hearing in a preliminary reference procedure. For the EDPS, this was an important step that may lead to a landmark decision on an issue that we have been following closely for a number of years.

The EDPS pleaded at the hearing of *Commission* v. *Hungary* (C-288/12). This case is the third infringement case on the independence of data protection

authorities, the other two being Commission v. Austria (C-614/10) and Commission v. Germany (C-518/07) for which rulings were given in 2012 and 2010 respectively.

Other cases in which the EDPS intervened are still pending, such as Pachtitis v Commission and EPSO (T-374/07), Pachtitis v Commission (F-35/08), ZZ v. EIB (Case F-103/11) as well as Dennekamp v. European Parliament (T-115/13).

In October 2013, the EDPS asked for leave to intervene in two further cases: Elmaghraby and El Gazaerly v. Council of the European Union (Case T-319/13) and CN v Parliament (Case T-343/13).

Cooperation

In the area of cooperation, we continued to actively contribute to the work of the Article 29 Working Party. In particular, we have been heavily involved as rapporteur or co-rapporteur for the Opinions on purpose limitation and on legitimate interest (key provisions subgroup), the Opinion on the smart grid data protection impact assessment template (technology subgroup) and the Opinion on open data (eGovernment subgroup).

Direct cooperation with national authorities is an area of increasing importance in the development of large-scale international databases such as EURODAC, the Visa Information System (VIS), the Schengen Information System II (SIS II) and the Customs Information System (CIS), which require a coordinated approach to supervision. In 2013, we provided the secretariat for the new SIS II Supervision Coordination Group (SCG) and we continued to chair the EURODAC, VIS and CIS SCGs.

Changes in coordinated supervision in 2013 were accompanied by challenges. The new EURODAC Regulation contained significant amendments, such as possible access by law enforcement authorities to EURODAC data. In addition, SIS II became operational. To reduce the financial, travel and administrative burdens, we established back to back meetings of the SCGs and aimed to ensure consistent, horizontal supervision policies of the large-scale IT systems where possible.

The SCG model will expand in 2014 with a new supervision coordination group for the Internal Market Information System (IMI). We consulted the national data protection authorities (DPAs) and the Commission in 2013 to take stock of the status and developments in the IMI Regulation in order to organise the first meeting for the group in 2014.

The coordinated supervision model has become a standard for the EU legislator and the Commission

has proposed it in a number of proposals such as those on Europol, smart borders, Eurojust and the European Public Prosecutor's Office.

Cooperation in international fora continued to attract attention, most notably the European and International Conferences of Data Protection and Privacy Commissioners. In 2013, the European Conference in Lisbon focused on the recent developments for the modernisation of the data protection frameworks of the EU, the Council of Europe and the OECD. In particular, the concepts of personal data, the rights of individuals on the internet and information security were discussed.

The International Conference was held in Warsaw and focused on the reforms of data protection all over the world, the interaction with technology and the roles and perspectives of different actors, including data subjects, data controllers and supervisory authorities.

Within the framework of the Council of Europe, the EDPS attended three meetings of the Consultative Committee of the Council of Europe Convention 108. It was particularly important for us to attend these meetings to be able to follow and influence the on-going modernisation of the Convention.

The EDPS also took part in the experts group tasked with updating the privacy guidelines of the Organisation for Economic Co-operation and Development (OECD).

We also gave significant input on data protection issues in many other important fora such as the Asia-Pacific Economic Cooperation (APEC), the French-Speaking Association of Personal Data Protection Authorities (AFAPDP) and the International Working Group on Data Protection in Telecommunications (The Berlin Group).

IT Policy

In terms of our IT policy, we contributed to several Opinions on Commission proposals, which are strategic in the future of the digital society in Europe, such as the Opinion of the Article 29 Working Party on smart grids, where the EDPS was rapporteur. Our IT expertise also resulted in the EDPS leading a visit to the EU Large-Scale Information Systems Agency in the context of SIS II migration. This expertise has been very useful in our supervision cases, including complaints, prior checks and inspections.

Key EDPS figures in 2013

→ 91 prior-check Opinions adopted, 21 non-prior check Opinions

→ 78 complaints received, 30 admissible

→ 37 consultations received on administrative measures

→ 8 on-the-spot inspections (including 2 fact finding visits) and 3 visits carried out

→ 1 set of Guidelines on the processing of personal data in the area of procurement

→ 20 legislative Opinions issued

→ 13 sets of formal comments issued

→ 33 sets of informal comments issued

Our exchanges with relevant staff in the EU administration in the preparation of our guidelines relating to data protection and technology issues have benefitted from this IT expertise; these exchanges have initiated discussions in the EU institutions on their general approach to risk assessment and security measures in light of the revelations of the weaknesses of widely used cryptographic and security tools.

Information & Communication

In the communication area, we increased the visibility of the EDPS at institutional level as we

carried out our three main roles: the supervisory, consultative, and cooperative. We use a number of indicators, such as the number of information requests from citizens, media enquiries and interview requests (press relations), the number of subscribers to our newsletter, followers of the EDPS account on Twitter, as well as invitations to speak at conferences and website traffic. These all support the view that we are increasingly a point of reference for data protection issues at EU level. There has been a consistent increase in the number of visits to the EDPS website over the year (63 % compared to 2012), the number of study visits has increased (17 groups, compared to two in 2012), as well as the number of requests for information and advice received from individuals (176 written enquiries translates to an increase of 51 % from 2012). In December, we launched a corporate page on LinkedIn which is another avenue to promote the EDPS as an institution, strengthen our online presence and enhance our visibility.

Internal organisation

Following the departure of the Head of Sector of Operations, Planning and Support after our records management system (CMS) had become operational in October 2013, we restructured our organisation chart so that the record management team now reports to the Director.

Further to the recommendations of the Internal Audit Service (IAS) and to increase efficiency, the Internal Control Coordinator's function was separated from the Human Resources Budget and Administration (HRBA) team and now also reports to the director.

Resource management

In 2013, we successfully increased our budget implementation rate. However, the final result fell short of our expectations because of the decision by the Court of Justice on the adjustment of salaries of EU staff. This unexpected decision was adopted late in the year, which left very little margin of manoeuvre to organise redeployment. Furthermore, the Council's refusal to consider any transfers to other lines from the salaries' budget reduced the margin further. If, as intended by the Commission, an agreement had been reached between the Council and the Parliament before the end of the year, the final implementation rate (84.7 %) would have been higher (87.2 %).

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) will help us to monitor and adjust, if needed, the impact of our work and the efficiency of our use of resources.

Here we report on the performance of our activities in 2013, 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 2013 (section 1.1).

Overall, the results show a positive trend in the performance of our activities. The implementation of the strategy is broadly on track and no corrective measures are needed at this stage.

The KPI scoreboard

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 will set the benchmark for coming years.

From left to right the members of the EDPS Management Board: Christopher Docksey, Director; Peter Hustinx, EDPS; Giovanni Buttarelli, Assistant Supervisor

KPIs	Description	Results 2013	Target 2013
KPI 1	Number of inspections/visits carried out. Measurement : compared to target	3 visits 8 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 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	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	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)	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	2013 as benchmark
KPI 7	Number of cases in which guidance is provided on technological developments. Measurement : compared to target	21	20
KPI 8	Number of visits to the EDPS website. Measurement : compared to previous year	293 029 (+63 % in comparison to 2012)	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 %
KPI 10	Rate of training implementation for EDPS staff. Measurement: number of actual training days divided by the number of estimated training days	85 %	80 %

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 of 2013 will determine the target for KPI number 4.

3. **Improve the good cooperation with Data Protection Authorities, in particular the WP29, to ensure greater consistency of data protection in the EU.**

   The results of 2013 will determine the target for KPI number 6.

   KPI number 7 refers to strategic objectives 1, 2 and 3. The target has been achieved.

4. **Develop a creative and effective communication strategy.**

   The results of 2013 will determine the target for KPI number 8.

5. **Improve the use of the EDPS human, financial, technical and organisational resources (through adequate processes, authority and knowledge)**

   KPIs numbers 9 and 10. The target for KPI number 10 has been achieved.

   We did not achieve the target for KPI number 9. In this respect, whilst we increased our budget implementation rate the final result fell short of the target, following the decision by the Court of Justice on the adjustment of salaries of EU staff. If the Court had approved the Commission's proposed approach, our final implementation rate (84.7 %) would have been higher (87.2 %) and would have achieved our target.

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.

Our guiding principles

1. We use our expertise and authority to exercise our supervision and enforcement powers. We aim to ensure the protection of personal information and a fair balance with wider policy and political objectives.
2. In our supervision and enforcement work:
   - we recognise that institutions – data controllers and DPOs/DPCs – carry first-line accountability;
   - we seek to help institutions carry out their responsibilities effectively, ensuring that the right support, training and guidance are in place;
   - we use our powers of supervision to reinforce responsibility;
   - we are willing to use our powers of enforcement where necessary.

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.

In 2013, as part of our regular supervision work, we paid particular attention to the action plan laid down in our Strategy 2013-2014. One of the points is to promote a *data protection culture* within the EU institutions and bodies so that they are aware of their obligations and are accountable for complying with data protection requirements.

In light of this, we continued to provide guidance and training to controllers, data protection officers (DPOs) and data protection controllers (DPCs) in the form of Guidelines on Public Procurement, Grants and External Experts; basic training for new DPOs on the prior checking procedure; special training for the DPOs of five EU Joint Undertakings. We also organised awareness raising initiatives within EU institutions and bodies by providing workshops for controllers at ETF and EDA and general workshops in the field of e-communication, the use of mobile devices in the workplace and on websites managed by EU institutions and bodies.

An important part of our work also focused on raising awareness of data protection at all levels of management, primarily by visiting those EU bodies where there has been a lack of communication or compliance with the data protection rules. Such visits generally comprise an on-site meeting with the EDPS or Assistant EDPS, resulting in a positive outcome: engagement of management and raised awareness of data protection.

Promoting dialogue with controllers, DPOs and DPCs is a key part of our support for the work of DPOs and gives us a better understanding of the constraints of institutions so that we can offer pragmatic advice. To this end, we held several meetings with controllers

either in the course of our prior check work or in the follow up to Opinions and decisions. The DPO network meetings, bilateral meetings and the helpline for DPOs were useful channels of communication for our work with the DPOs and DPCs.

As part of our compliance monitoring activities, we launched our fourth general stock taking exercise (Survey 2013) on 17 June 2013, the results of which are to be published early 2014. We also published a report compiling the results of the survey on the status of Data Protection Coordinators (DPCs) at the European Commission in January 2013.

This year also marked the adoption of our Inspection Policy, which sets out the main elements of the EDPS inspection procedure in order to provide guidance to all involved and ensure transparency to stakeholders. Based on the experience gained in our inspections work, we developed a comprehensive internal inspection manual to provide guidance to EDPS colleagues dealing with inspections.

Over the course of the year, our supervision activities in the field of prior checks, complaints and consultations on administrative measures remained a priority. The prior checking of processing operations which exhibit specific risks continued to be an important aspect of our supervision work in 2013. We saw a huge increase in the number of notifications received, as well as an increase in the number of Opinions adopted (91 Opinions, 21 non-prior check Opinions, 8 of these being joint Opinions covering 36 notifications).

The number of complaints received decreased, partly due to better information and awareness of EDPS competencies but also because of the effectiveness of our complaint submission form. In 2013, the EDPS received 37 consultations on administrative measures.

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 DPO. Some institutions have provided the DPO with an assistant or deputy DPO. The Commission has also appointed a DPO for the European Anti-Fraud Office (OLAF) in view of OLAF's independent function. A number of institutions have also appointed data protection coordinators or contacts (DPCs) in order to coordinate all aspects of data protection within a particular directorate or unit.

In 2013, five new DPOs were appointed, both in existing institutions and bodies and in new agencies or joint undertakings, bringing the total number of DPOs to 62 (the DPO of the European Central Bank acts also as DPO of the European Systemic Risk Board; CEDEFOP has two DPOs).

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 to meet in 2013.

A *DPO quartet* composed of four DPOs from the Council, the European Parliament, the European Commission and the European Food Safety Agency respectively, has been actively coordinating the DPO network. The EDPS continued to collaborate closely with this quartet.

The EDPS attended the DPO meeting held in March at the EMCDDA in Lisbon and hosted another one in Brussels in November. At these meetings, we took the opportunity to update the DPOs on our work and give an overview of recent developments in EU data protection. This year we focused in particular on the Data Protection Reform, developments at European and international level, updates on relevant court cases and relevant developments in EDPS activities such as the DPC and DPO status report, the EDPS guidelines and workshops and the end of the *ex-post* prior check notifications. The meetings were also an occasion for open discussions between DPOs and the EDPS on shared issues and common problems such as the processing of personal information related to the use of internet and communication networks and conflict of interests.

We organised a number of trainings and workshops for DPOs and DPCs in 2013 (see section 2.7 on Data Protection Guidance). In addition, one-to-one sessions took place between EDPS staff and some DPOs on their specific guidance needs. Further support to the work and role of DPOs was also provided by our involvement in the EIPA training and certification programme for DPOs.

Colleagues in our Supervision and Enforcement team also deal with telephone queries from DPOs and whenever possible provide immediate assistance and guidance on specific issues (more complex issues are dealt with in written consultations). In response to the increase in the number of telephone queries, we set up a helpline for DPOs which is available at set times in the week, when an EDPS member of staff answers questions over the phone. This initiative has been successful: it allows us to deal with simple questions in a quick and informal way and to provide specific guidance to DPOs. The direct helpline has also strengthened the cooperation and communication between us and the DPO community within the EU institutions and bodies.

2.3. Prior checks

2.3.1. Legal base

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 2013, we continued to apply the criteria developed in previous years[4] when interpreting this provision, both to decide whether a notification from a DPO is subject to a prior check or not and when advising on the need for the prior check of a consultation.

2.3.2. Procedure

2.3.2.1. Notification

When the EDPS receives an email notification from a DPO, in the standard EDPS format (Article 19 of the Rules of Procedure), we are obliged to carry out a prior check. The DPO must provide any additional information that relates to the notified processing operation in an annex to the notification form.

Prior checks involve operations not yet in progress, but also processing that began before 17 January 2004 (the appointment date of the first EDPS and Assistant EDPS) or before the Regulation came into force (*ex-post* prior checks). In such situations, an Article 27 check cannot be 'prior' in the strict sense of the word, but must be dealt with on an *ex-post* basis. When the EDPS started his activities, there was a backlog of *ex-post* prior check cases relating to processing operations already in place. It was, therefore, decided to accept *ex-post* notifications despite the absence of a legal basis for this practice.

In order to clear the backlog of *ex-post* prior check cases on 5 July 2012, European institutions and bodies were invited to ensure that all processing operations subject to prior checking were notified to the EDPS by the end of June 2013 (with the exception of certain activities carried out by newly established bodies that might be impossible to notify *ex-ante*, such as recruitment). As a result, the EDPS received 138 notifications from the beginning

4 See Annual Report 2005, section 2.3.1. on the EDPS website.

of June 2013 to the end of July 2013 (out of a total 272 notifications in 2013).

Consultations on the need for prior checks: When in doubt, the DPO can consult the EDPS on the need for prior checking under Article 27(3) of the Regulation. In 2013, we received 31 such consultations from DPOs.

CJEU

The DPO of the Court of Justice of the EU (CJEU) consulted the EDPS on the need to submit a notification for prior checking on three processing operations: IT general infrastructure, keeping of log files for IT applications and internet monitoring procedures. On the first two processing operations, we considered that they were not subject as such to prior checks as they concerned a variety of disaggregated processing operations to be analysed separately. For example, the IT infrastructure could be used for a number of different applications and purposes, such as for the email system, the case management system, internet, etc. Similarly, the log files may be kept and processed in a variety of different applications and circumstances.

However, we considered that the monitoring of internet use by CJEU staff was subject to a prior check as the purpose of the processing was to evaluate personal aspects and related potentially to suspected offences. We recommended that the examination of individual emails identifying the user be carried out only when there is reasonable suspicion of wrongdoing, corroborated by concrete initial evidence and in the framework of an administrative investigation.

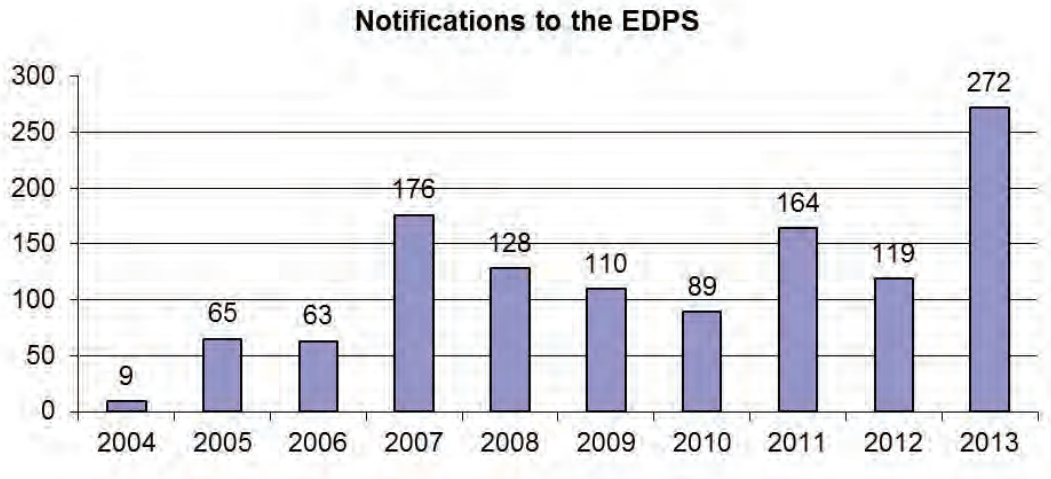
2.3.2.2. Period, suspension and extension

In accordance with Article 27(4) of the Regulation and Article 21 of the Rules of Procedure, the EDPS shall deliver an Opinion within two months following receipt of a notification[5]. This period of two months may be suspended until we receive any further information that we have requested. When the complexity of the matter so requires, the two month period may be extended once for a further two months. If the Opinion has not been delivered by the end of the period of two months, or any extension thereof, it shall be deemed to be favourable. To date, no such tacit Opinion has ever arisen. The starting date for calculating the deadline is the day following the date on which the notification form was received. If the final date is a public holiday or another day on which the EDPS services are closed, the next working day shall be considered the final date for delivering the Opinion

Prior to the adoption of an Opinion, we send a draft of that Opinion to the institution for feedback on the practical aspects and any factual inaccuracies, which is subject to a deadline of 10 days. This period may be extended upon a justified request from the controller. If no feedback is received within the deadline, the EDPS shall proceed with the adoption of the Opinion (Article 22 of the Rules of Procedure).

2.3.2.3. Register

In 2013, we received 272 notifications for prior checking (2 were withdrawn). Whilst we have cleared the backlog of *ex-post* prior checks for



5 *Ex-post* notifications are now dealt with within best possible delays, as the two months deadline for adopting an Opinion is not applicable.

most EU institutions, the deadline set to clear all *ex-post* notifications, other processing operations put in place by EU agencies, in particular by newly established ones, the follow-up of Guidelines issued, and several visits to agencies in 2013 have generated a considerable increase in the number of notifications.

Under the Regulation, we must keep a register of all prior check processing operations for which we have been notified (Article 27(5)). This register contains the information referred to in Article 25 and the deadline for implementing the recommendations from our Opinions. In the interests of transparency, the register is available to the public on our website (except for security measures, which are not mentioned in the public register).

2.3.2.4. Opinions

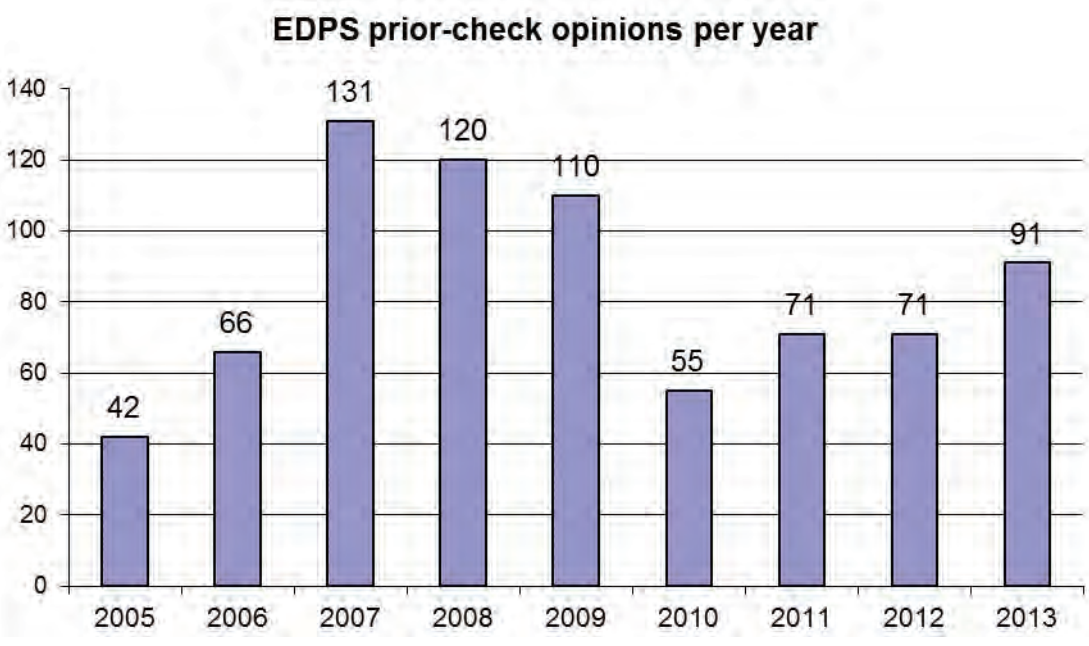
Our final position on a processing operation is outlined in an Opinion, which is notified to the controller of that operation and the DPO of the institution or body (Article 27(4)). In 2013, we issued 91 prior check Opinions and 21 Opinions on 'non-prior checks' (see Section 2.3.4). These figures take into account that we dealt with a significant number of cases by issuing joint Opinions: in 2013, we issued 8 joint Opinions (3 of which were for non-prior check cases) responding to a total of 36 notifications.

In 2013, we continued to address the majority of our Opinions to EU agencies and bodies. EU agencies have continued to notify their core business activities and standard administrative procedures according to the relevant EDPS procedures (see Section 2.3.2.1).

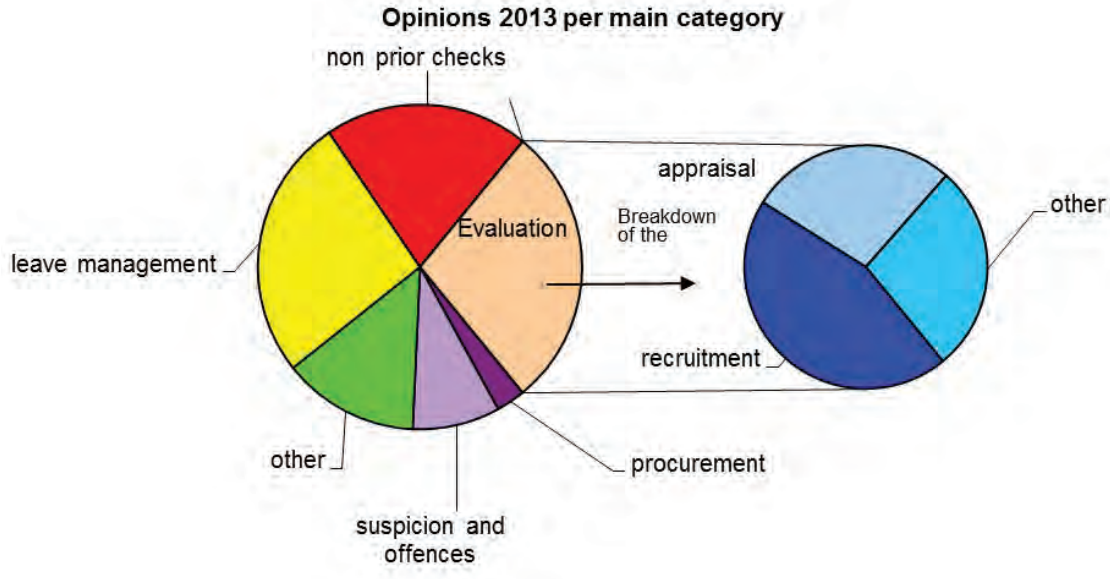
Opinions routinely contain a description of the proceedings, a summary of the facts and a legal analysis of whether the processing operation complies with the relevant provisions of the Regulation. Where necessary, we include recommendations to enable the controller to comply with the Regulation. In the concluding remarks, the EDPS usually states that the processing does not seem to involve a breach of any provision of the Regulation, provided these recommendations are taken into account, but we may of course exercise other powers granted to us under Article 47 of the Regulation.

Once we have delivered our Opinion, it is made public. All our published Opinions are available on our website in three languages (as these become available), in most cases together with a summary of the case.

A case manual ensures that the entire team follows the same approach and our Opinions are adopted after a complete analysis of all significant information. The manual provides a template for Opinions, based on accumulated practical experience and is regularly refined and updated. In addition, we use a workflow system to make sure that all recommendations in any given case are followed up and, where applicable, all enforcement decisions are complied with (see Section 2.3.6).



2.3.3. Main issues in prior checks



2.3.3.1. Purpose limitation / compatible use

Several cases analysed in 2013 relate to the definition of compatible use and demonstrate a possible trend in the further use of information that was originally collected for another purpose. The concept of purpose limitation is an essential first step in applying data protection law. Purpose limitation means that personal information may only be collected for specified, explicit and legitimate purposes. The concept contributes to transparency, legal certainty and predictability and aims to protect individuals by setting limits on how their information is used.

A notification by the European Food Safety Authority (EFSA) allowed us to clarify the compatible use of information originating from an access control system. The EFSA intended to use access badge information for controlling staff presence in the office. Whilst the EDPS reply of 9 April 2013 concluded that this particular operation was not subject to a prior check, we highlighted the importance of the purpose limitation principle. This means that in each situation where the further use of personal information is considered, a distinction must be made between additional uses that are 'compatible' and other uses, which are considered 'incompatible'. For instance, the potential to link an access control database with a time management database would not be compatible because it implies a structural change of purpose. In the case of EFSA, the use could be considered compatible in view of helping jobholders by facilitating the recording of flexitime. However, we expressed doubts as to the necessity of implementing such a system, as other means are available that do not require the use of records from the access control system.

The European Investment Bank (EIB) consulted us on the legality of analysing information from an access security system or from a time management system for another purpose, namely for investigations to instruct disciplinary procedures. In our Opinion of 17 April 2013, we stressed the purpose limitation principle, but also noted that it offered a degree of flexibility to the EIB. Following an analysis of the rules governing disciplinary procedures and fraud investigations at the EIB, we concluded that the following limitations apply when the EIB uses such information in disciplinary investigations:

- such use must be limited to the purposes of disciplinary procedures and fraud investigations at the EIB and the proportionality and necessity of the processing of the information must be respected;
- the re-use of this information for another purpose is only permitted in the context of an open disciplinary process for a specific case and must not serve as an opportunity for a fishing opera-

tion (an attempt to discover the facts about something by collecting a lot of information, often on unrelated or minor matters or in secret).

2.3.3.2. eCommunication and eMonitoring

In a number of cases, the EDPS was notified of or consulted on processing operations that involved eCommunication and eMonitoring.

In a consultation on call monitoring of data stemming from the unified communication system (UniComm) at the European Union Agency for Fundamental Rights (FRA), we clarified the type of electronic communications cases that need to be notified to us for prior checking. In our reply of 1 February 2013, the EDPS established the principle that electronic communications (and in particular the processing of telephone records) are subject to prior checking under three conditions:

1. if there is a structural breach of confidentiality of communication; or
2. the processing relates to suspected offences or security measures; or
3. it is intended to evaluate personal aspects relating to individuals.

In the FRA case, it appeared that the personal information in question is processed only to ensure the good functioning, identification and handling of security threats against the Unicomm system. Similarly, the processing does not appear to violate the confidentiality of communications, as certain traffic information is processed solely to allow individuals to identify their private calls with no interference to the content of their communications. We concluded, therefore, that the processing operation was not subject to a prior check.

We also thoroughly reviewed an email monitoring policy in place at the European Railway Agency (ERA), which was drawn up to help prevent disruption and misuse by staff and recommended amendments in a number of areas. In our reply to the prior check notification, we highlighted the following fundamentals:

- any email monitoring must be necessary and proportionate;
- it should be performed first by automated means and on a no-name basis;
- individual emails identifying the user must only be examined when there is reasonable suspicion of wrongdoing, corroborated by concrete initial evidence and in the framework of an administrative investigation.

Among other things, we invited ERA to exclude the applicability of the email policy to personal webmail accounts and to exclude, or significantly limit, ERA's power to interfere with personal communications.

A second case involving the European Railway Agency (ERA) regarded eMonitoring for the purpose of verifying whether internet use is in conformity with documented internal policy. In our prior check Opinion, we applied the guidance outlined in our previous Opinions, highlighting the following points:

- the general monitoring of individual internet use in the absence of suspicion is excessive;
- a policy should allow for a gradual increase in monitoring depending on concrete needs and circumstances;
- monitoring internet use of identified, individual users should only take place if there is reasonable suspicion, corroborated by evidence and in the framework of an administrative inquiry;
- before engaging in individual monitoring, other less intrusive measures (such as general reminders or warnings) should be considered where possible.

2.3.3.3. Transfers of data

The issue of transferring data to internal and external recipients, for instance in security investigations and in case of fraud and financial irregularities in the management of EU funds, was a recurring topic in cases dealt with in 2013.

On 1 February 2013, we published our first prior check Opinion on a European External Action Service (EEAS) processing operation. This prior check related to security investigations carried out by the EEAS Division for Security and Security Policy. The original EEAS notification covered various security measures, which were clarified and limited in scope over the course of our examination.

In our conclusions, we recommended that the proposed security policy be amended. Another recommendation related to transfers of data - as an external service, this could include transfers to third countries and international organisations - and we referred to our forthcoming paper on data transfers.

At the Joint Research Centre (JRC) in Petten, a Commission Security Decision defines the general tasks of the Security Service. In the light of its revision and an upcoming Memorandum of Understanding between the Directorate General Human Resources & Security Directorate of the European Commission and the JRC to conduct certain types of security investigations, the JRC notified the EDPS of processing operations carried out in security investigations. The purpose of the processing operation is to obtain information associated with security related incidents such as traffic accidents, parking violations and vandalism that have occurred on JRC Petten premises, ultimately resulting in a report describing the occurrence.

The main concerns that we outlined in our Opinion of 19 March 2013, related to the transfer of data to recipients such as EU institutions or bodies or national authorities (police and judicial, for instance) and the use they might make of them. We suggested that a notice on purpose limitation be provided to these recipients and that the necessity of a potential transfer of information be duly assessed and documented before any actual transfer takes place.

The Investigative Data Consultation Platform (IDCP) is a project database, which aims to facilitate cooperation and exchange of information on anti-fraud investigations between OLAF and its international partner authorities. The IDCP contains a subset of data from the investigative files of OLAF and its selected international partners (IDCP partners). The purpose of the tool is to allow IDCP users to identify and exchange relevant investigation-related information. It is OLAF's intention that the IDCP should work essentially as a locator of basic investigation-related information. By consulting the subset of data stored in the IDCP, the partner will be able to identify whether any other authority possesses information relevant for its investigation and to submit a specific request for cooperation in accordance with the applicable administrative cooperation arrangement.

OLAF notified the IDCP to the EDPS in March 2012 for prior checking well before finalising its implementation. The analysis of the processing operation under Article 27 and its development proceeded more or less in parallel.

After a thorough assessment, we concluded that the proposed processing operation must be subject to a number conditions and limitations for it to fully respect the Data Protection Regulation (EC) 45/2001. Among other things, we recommended:

- clearly specifying the responsibilities of OLAF and other IDCP partners to respect the requirements of the Regulation;
- significantly limiting the conditions and modalities of the database consultation to comply with the principles of necessity and proportionality;
- ensuring sufficiently frequent (at least annual) reviews of the accuracy, completeness and up-to date nature of the personal data included in the IDCP;
- performing a complete analysis of the risks and defining in detail the specific security controls that need to be implemented to reduce the risks to a level acceptable to OLAF's management.

Furthermore, we required OLAF to apply for a separate authorisation for the purposes of Article 9(7) of the Regulation. This authorisation aims to verify that sufficient privacy and data protection guarantees are in place.

2.3.3.4. Miscellaneous

The aim of the European Investment Bank's implementation of anti-money laundering (AML) and combating the financing of terrorism (CFT) controls is to apply best banking practices in these fields and to minimise the risks to integrity and reputation.

In our prior check Opinion, we urged the EIB to reinforce the existing legal basis. We further stressed the need to introduce a number of safeguards to enhance the quality of the personal data processed. Personal information which has no relevance to the underlying objective should not be processed. Unverified rumours, press reports, or other allegations should be treated with care. Ultimately, the EIB should put in place procedures to ensure that the information used is accurate and up-to-date.

On 8 March 2013, the European Joint Undertaking for ITER and the Development of Fusion Energy (F4E) notified us of its processing operations on the declarations of interests of the members of its Executive Committee. Such declarations safeguard the independence of these members and avoid any conflicts of interest which could interfere with their activities. These declarations of interests can be made public upon request. In our Opinion of 30 May 2013, we said that such publication can be justified to allow control by peers and the public depending on the tasks of the members of the Executive Committee. Institutions and bodies should assess the potentially public nature of personal information when collecting it and properly inform the individuals concerned about its possible disclosure.

We also pointed out that the disclosure of declarations of interest is in effect a transfer of data. As set out in the EDPS paper on Public access to documents containing personal data after the Bavarian Lager ruling, an institution needs to take into account the legitimate interests and views of the individual(s) concerned in order to balance the interests of all concerned and make a well-informed decision. In our view, consent is not necessary as the balance of interests in this instance would be devoid of substance otherwise. Nevertheless, individuals have the right to object to the publication on compelling and legitimate grounds.

2.3.4. Notifications withdrawn or not subject to prior checking

41 cases were found not to be subject to prior checking in 2013. In such situations, also referred to as *non-prior checks*, the EDPS may still make recommendations. In addition, two notifications were withdrawn and one replaced. The significant increase of inappropriately submitted cases (compared to 8 in 2012) is a consequence of the deadline established by the EDPS to clear the backlog of *ex-post* prior checking cases (see paragraph 2.3.2.1). Most of the cases not subject to prior checking were submitted just before the deadline.

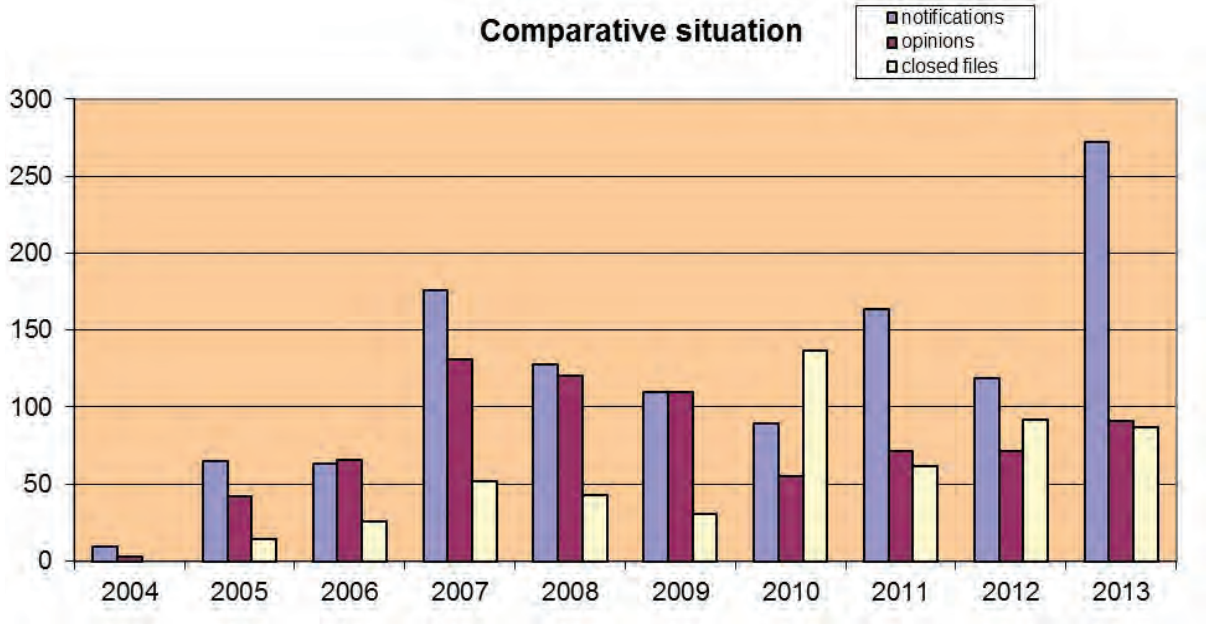
Sometimes, we need to request the controller to withdraw a notification where the information submitted is incomplete, inaccurate or misleading. In 2013, two notifications were withdrawn and replaced at our request. The first notification was not aligned with previous prior check notifications on similar processing operations, the purpose of the processing was not clearly described and no precise legal basis was referred to. In the second case, we required the controller to withdraw the initial prior check notification because during the development phase, the notified project was subject to substantial modification compared to the description contained in the notification.

2.3.5. Follow-up of prior checking Opinions

*An EDPS prior check Opinion usually concludes with a statement that the processing operation does not violate the Regulation providing certain **recommendations** are implemented. Recommendations are also issued when a case is analysed to verify the need for prior checking and some critical aspects appear to deserve corrective measures. The EDPS allows the institution three months from the date of the Opinion to give feedback on the implementation of the recommendations made in the Opinion. Should the controller not comply with these recommendations, the EDPS may exercise the powers granted to him under Article 47 of the Regulation.*

To date, institutions and bodies have chosen to follow our recommendations and there has been no need for us to open enforcement proceedings. In the formal letter that accompanies an Opinion, we request that the institution or body concerned informs us of the measures taken to implement our recommendations within a threemonth period.

As outlined in the Rules of Procedure (Article 25.2), we consider this follow-up a critical element in achieving full compliance with the Regulation. In keeping with our 2010 Policy Paper on Monitoring and Ensuring Compliance with Regulation (EC) No 45/2001, we expect institutions and bodies to be accountable for any recommendations we make.



This means that they bear the responsibility for implementing them and they must be able to demonstrate this to us. Any institution or body failing to act on the recommendations will thus risk formal enforcement action.

2.3.6. Conclusions

The 91 prior check Opinions issued have provided valuable insight into the processing operations of the European administration and have enabled us to provide recommendations that will better guarantee the fundamental right to data protection of individuals in a consistent way. The importance of this activity lies in the potential it gives us to check compliance with data protection rules before the processing activity is put into place.

This check is carried out in cases of specific risks that are selected according to the criteria developed by the Regulation. This approach of selectivity in our supervision function allows us to concentrate on those cases where fundamental rights might be put at risk and play a preventive and precautionary role.

In terms of follow-up of our prior check Opinions, we closed 87 cases in 2013. We will continue to closely monitor and follow-up our recommendations to ensure that institutions and agencies integrate them in a timely and satisfactory manner.

2.4. Complaints

2.4.1. The EDPS mandate

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).

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 not admissible.

Complainants must also identify themselves so anonymous requests cannot be 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.).

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, to modify the content of the documents that the complainant wants to challenge or to grant financial compensation for damages.

A Czech citizen complained about national court proceedings concerning restitution of his property. As no processing of personal data by EU institutions was involved, no inquiry of these complaints was carried out.

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.

A Greek citizen complained to the EDPS explaining that he had addressed the Greek data protection authority (who had not replied to him) to check compliance of a decision taken by a national public sector body with the Greek data protection laws. The complainant asked the EDPS to intervene in the case. We explained that the EDPS has no power to take action against national data protection authorities, as our competence is limited to the processing of personal data by EU institutions or bodies.

2.4.2. Procedure for handling of complaints

The EDPS handles complaints according to the existing legal framework, the EDPS Rules of Procedure and the general principles of EU law and good administrative practice common to the EU institutions and bodies.

In all phases of handling a complaint and in accordance with Article 33 of the Rules of Procedure, the EDPS adheres to the principles of proportionality and reasonableness. Guided by the principles of transparency and non-discrimination, we undertake appropriate actions taking into account:

- the nature and gravity of the alleged breach of data protection rules;
- the importance of the prejudice that one or more data subjects may have suffered as a result of the violation;
- the potential overall importance of the case in relation to the other public and/or private interests involved;
- the likelihood of proof that the infringement has occurred;
- the exact date of the events, any conduct which is no longer yielding effects, the removal of these effects or an appropriate guarantee of such a removal.

In February 2011, we updated the way complaints can be submitted to us by offering an **online complaint submission form** in English, French and German on our website. This form helps complainants to assess the admissibility of their complaint and thereby to submit only relevant matters to the EDPS. It also allows us to analyse more complete information in order to speed up the processing of complaints and to reduce the number of manifestly inadmissible complaints.

A complaint must identify the person making the complaint. It must also be submitted in writing in an official language of the EU and provide all information necessary to better understand the subject matter. Each complaint received by us is carefully examined. The preliminary examination of the complaint is specifically designed to verify whether a complaint fulfils the conditions for further inquiry, including whether there are sufficient grounds for an inquiry.

Our **internal manual** was designed to provide guidance to staff when handling complaints. We have also implemented a **statistical tool** designed to monitor complaint-related activities, in particular to monitor the progress of specific cases.

A complaint which concerns a matter outside our **competence** is declared inadmissible and the complainant is informed accordingly. If relevant, we will also inform the complainant of any other competent bodies (e.g. the Court, the Ombudsman, national data protection authorities, etc.) to whom the complaint can be submitted.

A complaint that addresses facts which are **clearly insignificant**, or would require **disproportionate** efforts to investigate is not pursued. We can only investigate complaints that concern a **real or potential** - and not a purely hypothetical - breach of the relevant rules relating to the processing of personal information. This includes a study of alternative options to deal with the relevant issue, either by the complainant or by us. For instance, we can open an inquiry into a general problem on our own initiative as well as open an investigation into an individual case submitted by a complainant. In such cases the complainant is informed about all available means of action.

A complaint is, in principle, **inadmissible** if the complainant **has not first contacted the institution concerned** in order to redress the situation. If the institution was not contacted, the complainant should provide the EDPS with sufficient reasons for not doing so.

If a matter is already being examined by an administrative body, for instance, an internal inquiry by the institution concerned is in progress, the complaint is, in principle, still admissible. However, we can decide, on the basis of the specific facts of the case, to await the outcome of the administrative procedure(s) before beginning our investigation. On the contrary, if the same matter (same factual circumstances) is already being examined by a Court, the complaint is declared inadmissible.

In one complaint case regarding an administrative inquiry against a member of staff, the complainant initiated a procedure under Article 91 of the Staff Regulations after having filed a complaint with the EDPS.

The EDPS decided to suspend his complaint case as a consequence.

In order to ensure the consistent treatment of complaints concerning data protection and to avoid unnecessary duplication, the European Ombudsman and the EDPS signed a Memorandum of Understanding (MoU) in November 2006. If a complaint relating to the same facts has been lodged with the European Ombudsman, the EDPS will examine its admissibility in the light of the MoU. The MoU stipulates, amongst other things, that a complaint that has already been examined should not be reopened by another institution unless significant new evidence is submitted.

According to Article 32.3 of our Rules of Procedure, there is a **time limit** for lodging a complaint. A complaint shall, in principle, only be lodged within two years of the date on which the complainant had knowledge of the facts on which it is based.

Where a complaint is admissible, we will launch **an inquiry** to the extent appropriate. This inquiry may include a request for information to the institution concerned, a review of relevant documents, a meeting with the controller or an on-the-spot inspection. The EDPS has the authority to obtain access to all personal information and to all information necessary for the inquiry from the institution or body concerned. We can also obtain access to any premises in which a controller or institution or body carries out its activities.

At the end of the inquiry, a **decision** is sent to the complainant as well as to the controller responsible for processing the information. In the decision, the EDPS expresses his view on a possible breach of the data protection rules by the institution concerned. The **competence of the EDPS** is broad, ranging from giving advice to data subjects, to warning or admonishing the controller, to imposing a ban on the processing or referring the matter to the Court of Justice.

Any interested party can ask for a **review** of the EDPS' decision. A request for review must be lodged within one month of the date of receipt of the decision and is limited to new elements or legal arguments which have not been taken into account by us. Independently of a possible request to review our decision, the decision can also be challenged before the Court of Justice of the European Union in accordance with the conditions laid down in Article 263 TFEU.

No decisions of the EDPS were challenged before the Court in 2013.

2.4.3. Confidentiality guaranteed to the complainants

The EDPS recognises that some complainants put their private lives or careers at risk when exposing violations of data protection rules and that ***confidentiality*** *should, therefore, be guaranteed to the complainants and informants who request it. On the other hand, the EDPS is committed to working in a* ***transparent manner*** *and to publishing at least the substance of his decisions. The internal procedures of the EDPS reflect this delicate balance.*

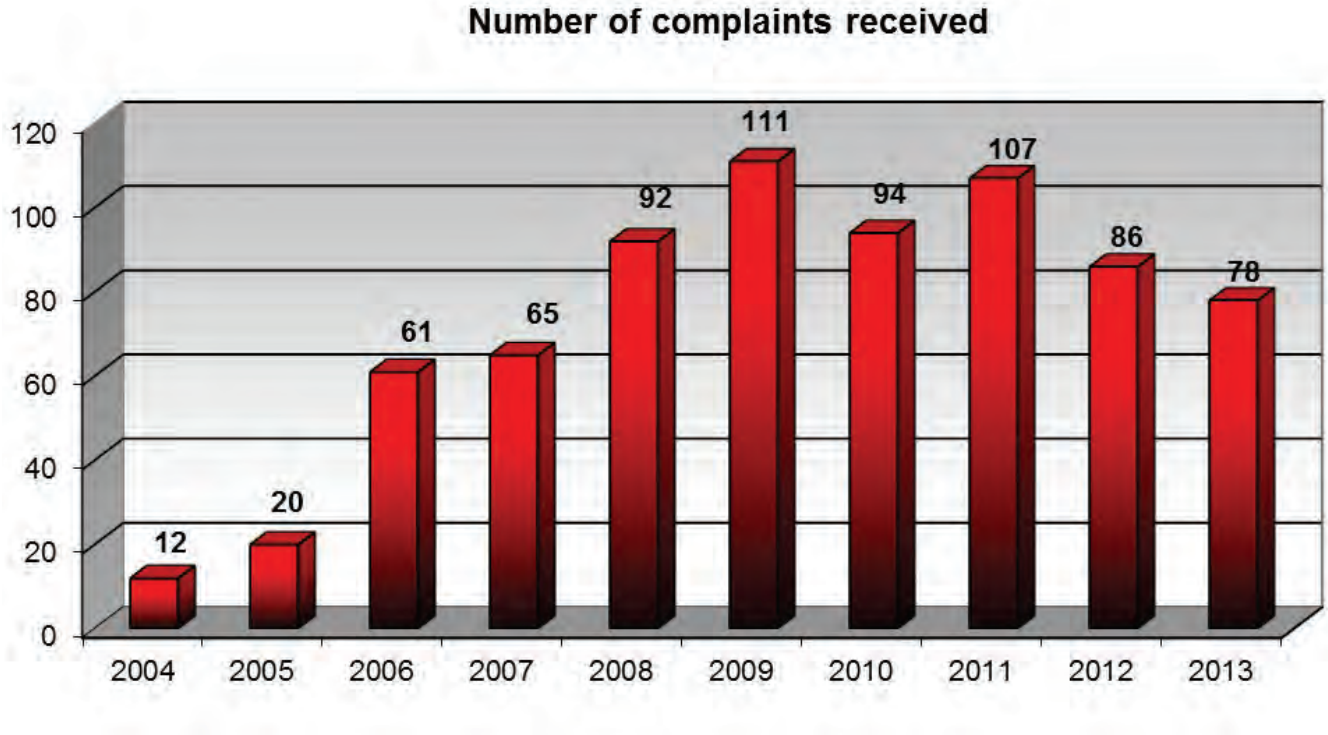
As standard policy, complaints are treated confidentially. **Confidential treatment** implies that personal information is only used by us to handle the complaint. However, for the proper conduct of the investigation it is usually necessary to inform the relevant services of the institution concerned and, if necessary for the investigation, the third parties involved, about the content of the complaint and the identity of the complainant. In accordance with Article 33.3 of our Rules of Procedure, the EDPS shall disclose the content of a complaint and the identity of the complainant only to the extent necessary for the proper conduct of the inquiry. We also copy the DPO of the institution concerned in all correspondence between us and the institution.

If the complainant requests **anonymity** from the institution, the DPO or third parties involved, he is invited to explain the reasons for such a request. We will then analyse the complainant's arguments and examine the consequences for the viability of our subsequent inquiry. If we consider that the anonymity of the complainant is not appropriate, we will explain our evaluation and ask the complainant whether he accepts our examination of the complaint without guaranteeing anonymity or whether he prefers to withdraw the complaint.

If the complainant decides to withdraw the complaint, the institution concerned is not informed of the existence of the complaint. In such a case, we may undertake other actions on the matter, without revealing the existence of the complaint to the institution concerned, for instance, an inquiry on our own initiative or a request for notification about a data processing operation.

During and on completion of an inquiry, all **documents related to the complaint**, including the final decision are not disclosed by us to third parties unless the EDPS is under a legal obligation to do so.

2.4.4. Complaints dealt with in 2013



2.4.4.1. Number of complaints

In 2013, the EDPS received 78 complaints, a decrease of approximately 9 % compared to 2012, confirming the effectiveness of the online complaint submission form available on our website in reducing the number of inadmissible complaints. Of these, 48 complaints were inadmissible, the majority relating to processing at national level as opposed to processing by an EU institution or body.

The remaining 30 complaints required in-depth inquiry, a decrease of about 25 % compared to 2012. In addition, 20 admissible complaints, submitted in previous years (two in 2009, one in 2010, four in 2011 and 13 in 2012), were still in the inquiry, review or follow-up phase on 31 December 2013.

2.4.4.2. Nature of complainants

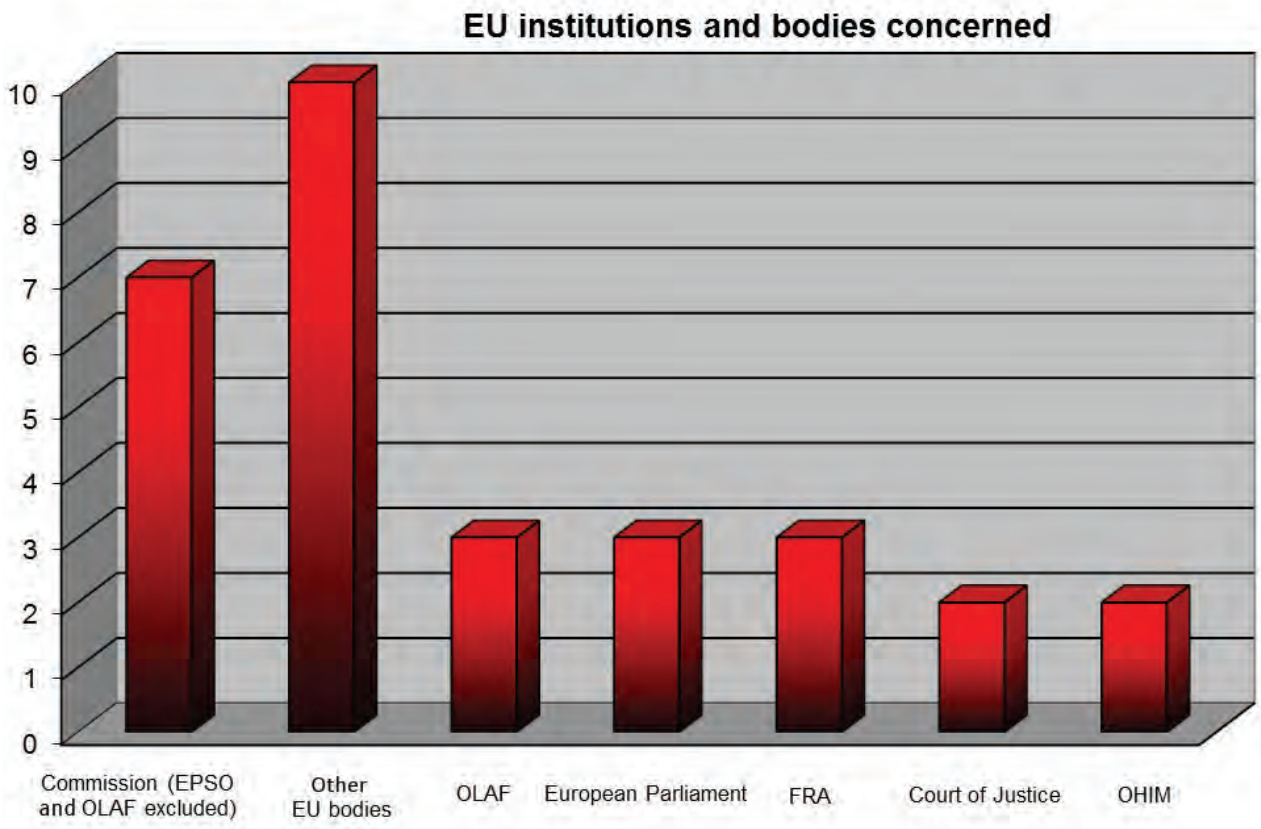
Of the 78 complaints received, 23 complaints (29 %) were submitted by staff of EU institutions or bodies, including former staff members and candidates for employment. The complainant did not appear to have an employment relationship with the EU administration in the remaining 55 complaints.

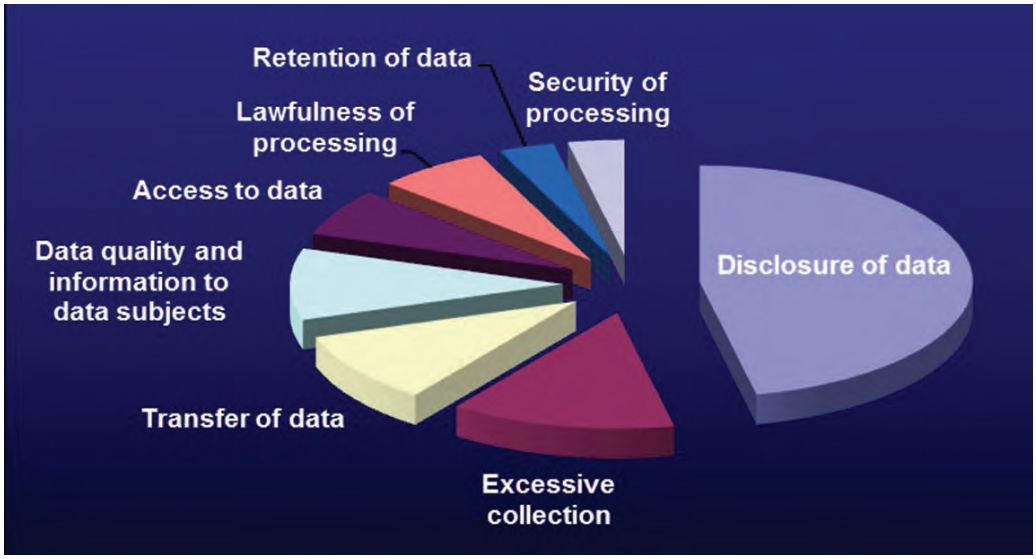
2.4.4.3. Institutions & number of complaints

Of the 30 admissible complaints submitted in 2013, most were directed against the European Commission, OLAF and the European Parliament. This is to be expected since the Commission and the Parliament conduct more processing of personal information than other EU institutions and bodies. The relatively high number of complaints against OLAF may be explained by the nature of the activities undertaken by this body. However, a significant number of complaints were also directed against the Fundamental Rights Agency.

2.4.4 .4. Language of complaints

The majority of complaints were submitted in English (50 %), German (17 %), French (15 %) and Italian (8 %). Complaints in other languages are relatively rare (10 %).





2.4.4.5. Types of violations alleged

The violations of data protection rules alleged by the complainants in 2013 related mainly to:

- Disclosure of data (47 %), a breach of data subjects' rights, such as excessive collection of personal information (13 %), transfer of data (10 %), data quality and information to data subjects (10 %);
- Access to data (7 %), lawfulness of processing (3 %) and retention of data (3 %).

2.4.4.6. Results of EDPS inquiries

In four cases resolved in 2013, the EDPS found that there was no breach of data protection rules or that the necessary measures had been taken by the data controller during the EDPS inquiry.

Conversely, non-compliance with data protection rules was found in six cases and recommendations were addressed to the controller.

The EDPS received a complaint about access to the personal data of a person who had since left the institution and about the conservation of that same data in a database for a period longer than necessary for the purposes for which it was collected. The EDPS considered that the institution was in breach of the Regulation for having failed to adopt adequate technical and organisational measures for ensuring that the complainant's personal information was not unlawfully accessed and for not deleting the data after a certain period.

In two cases, allegations reported to the EDPS in the context of a complaint led to a decision to launch a broader, fact-finding visit to the premises of the EU institution concerned.

2.5. Monitoring compliance

The EDPS is responsible for monitoring and ensuring the application of Regulation (EC) No 45/2001. Monitoring is performed through periodic general surveys. In addition to this general stock taking exercise, 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. In 2013, 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. General monitoring and reporting 2013 Survey: Survey on the function of the Data Protection Coordinator at the European Commission and General Report

Over the past few years, some of the larger institutions have established networks of DPCs to act as a relay for the Data Protection Officer locally. The European Commission launched its network in 2002 which in principle now involves all DGs.

In June 2012, we launched a survey on the function of the DPC at the Commission. A report of our findings was published in January 2013.

The findings reveal a great disparity between the resources allocated to the function by the DGs: between 5 % and 100 % of a DPC's time is assigned to his/her function as DPC. However, all DPCs have a common series of basic tasks which they are

required to perform irrespective of the time available to do so. Accordingly, one of the first conclusions of our report is the need to establish minimum criteria to be satisfied by DGs in order to preserve the useful nature of the role.

Among other things, our conclusions also make reference to:

- the appointment decision that should mention the minimum duration of the term of office;
- a specific reference to the role of DPC in the job description;
- the guarantee of the necessary resources such as time to attend DPC network meetings; and
- the inclusion of DPC responsibilities in the individual's appraisal.

In addition, the report outlines the good practices developed in certain DGs, such as creating a functional mailbox that can be used to consult the DPC, developing an intranet page devoted to data protection, making sure the role of DPC is visible in the organisational chart or structuring the DPC's access to his superiors and ensuring that he is kept informed effectively.

We used the report to express the EDPS' support for the DPC function, which contributes to good governance. The DPCs, whose function is recognised internally, contribute to making DGs more accountable for data protection, a key concept in the current data protection reform.

On 17 June 2013, we initiated our fourth general stock taking exercise, Survey 2013, to ascertain the progress made in the implementation of the Regulation in all 62 institutions and bodies. In addition to the issues analysed in previous surveys (level of notifications to the DPO, level of prior checks, etc.) we requested information on:

- the data protection training given to staff;
- contractual clauses for processors;
- involvement of the DPO in designing new processing operations; and
- transfers to recipients not subject to national provisions implementing Directive 95/46.

General surveys allow us to identify underperforming bodies and take specific actions to address the problems. The results of the survey will be published in early 2014.

2.5.2. Visits

At the EDPS, we promote the notion of accountability, but also take action where necessary. A visit is a typical way for us to take targeted action. A visit is a compliance tool, the aim of which is to engage the commitment of the senior management of an institution or agency to comply with the Regulation.

The decision to visit is usually taken when there has been a lack of compliance with the data protection rules, a lack of communication or simply to raise awareness. This is based on the information we have gathered when monitoring compliance, for example, in a general survey. 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 body visited.

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
- generally fostering better cooperation with the agencies visited.

In the course of 2013, we visited two EU agencies, ESMA and EIGE. A working-level meeting took place with eu-LISA.

ESMA

The European Securities and Markets Authority (ESMA) in Paris, became operational on 1 January 2011. Although we were consulted on the implementing rules for the DPO function, a DPO was only appointed in Spring 2013 and no prior check notifications had been submitted before then. To raise the profile of data protection at ESMA, a meeting between the Assistant Supervisor and the Executive Director of ESMA as well as the newly-appointed

DPO took place in Brussels in April 2013. Following the meeting, ESMA significantly increased its compliance efforts and now performs on a level similar to other recently established agencies.

EIGE

The European Institute for Gender Equality (EIGE) in Vilnius, officially became operational in Summer 2010. EIGE replied late to our 2011 general survey and by early 2013, had not submitted a single prior check notification. For this reason, the Assistant Supervisor visited EIGE in May 2013. The half day visit consisted of meetings with management, the staff in charge of processing operations, as well as the DPO and Deputy DPO. Following the visit, EIGE and the EDPS agreed on a roadmap towards full compliance. So far, EIGE has complied with the steps of the roadmap and now shows better compliance than many other recently established agencies.

eu-LISA

The EU Agency for the operational management of large-scale IT systems (eu-LISA) is currently in charge of the operational management of EURODAC, VIS and SIS II and became operational in December 2012. While its headquarters are in Tallinn, technical staff and the main data centre are based in Strasbourg. In May 2013, staff members of the EDPS conducted a working-level visit to the agency's Strasbourg facilities in order to get an overview of activities, collect information on security measures and to be updated on the state of play of the migration to the new version of the Schengen Information System. This was not a management-level visit triggered by compliance issues, but a working-level meeting to foster good cooperation and technical insight into the operations of the new EU agency.

We continued to follow-up on past visits and on the implementation of roadmaps. The European Training Foundation (ETF) in particular demonstrated active cooperation with us in adopting concrete measures to implement recommendations agreed in the roadmap.

2.5.3. Inspections

Inspections are another important tool that allows the EDPS to monitor and ensure the application of the Regulation. They are provided for under its Articles 41(2), 46(c) and 47(2).

The EDPS has 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. These powers ensure that the EDPS has sufficient tools to perform his function.

Inspections can be triggered by a complaint or take place at the EDPS' own initiative.

Article 30 of the Regulation requires EU institutions and bodies to cooperate with the EDPS in performing his duties and to provide the information and access requested.

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

In November 2013, the EDPS adopted a comprehensive inspection manual to provide guidance to EDPS staff dealing with inspections. The document contains a description of the administrative procedure, inspectors' tasks, security considerations for inspections, and standard forms for producing inspection documents. The manual is complemented by an inspection policy and inspection guidelines. The inspection policy sets out the main elements of the EDPS inspection procedure in order to give guidance to all involved and ensure transparency to stakeholders. The inspection guidelines, which are sent to the relevant institution prior to an inspection, provide a link between the policy and the manual and outline both operational and legal issues.

In 2013, we continued the follow-up of previous inspections. We inspected EMA in June 2013 and conducted targeted, on-the-spot inspections were conducted in July at four Luxembourg-based EU institutions and bodies on the way they inform the general public about video-surveillance on their premises. We also carried out an OLAF-CIS-MAB-FIDE inspection and performed two fact-finding visits.

EMA inspection

In June 2013, we inspected the European Medicines Agency (EMA) in London, focusing on two processing operations: EudraVigilance, one of EMA's core business systems and video surveillance on EMA's premises. EudraVigilance was selected for two reasons: firstly, because the database is likely to contain vast quantities of sensitive medical data, and secondly, to speed up the follow-up of a prior check issued.

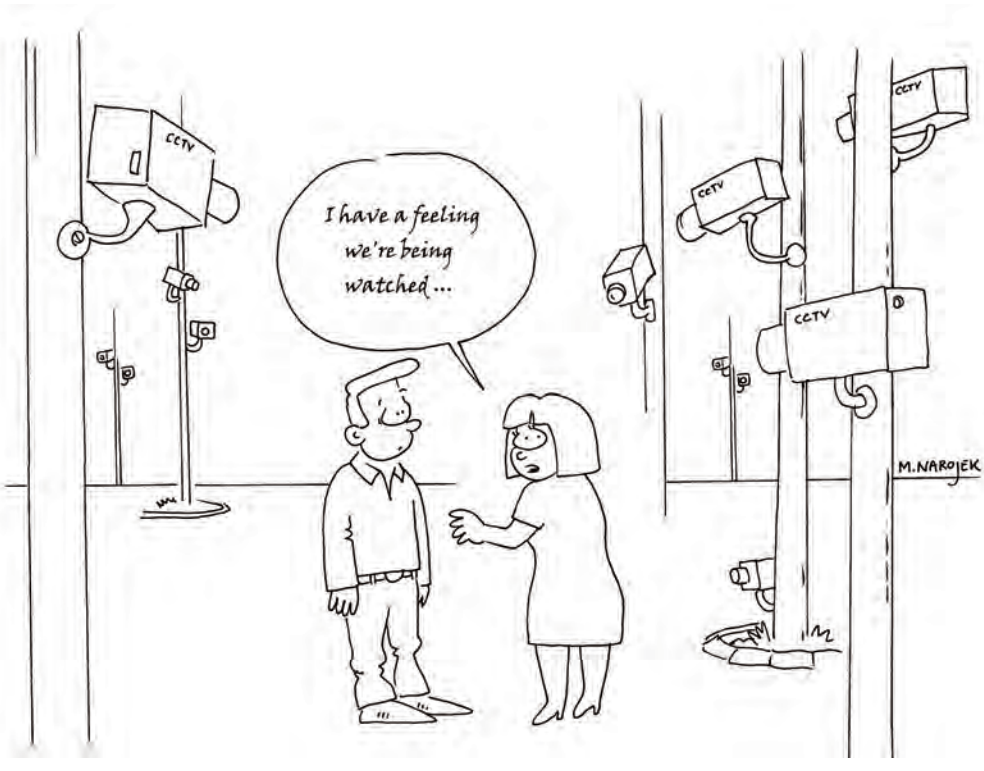
EudraVigilance stores information on adverse reactions to medicines, both those authorised in the EU and those used in clinical trials. Its purpose is to discover new side effects and other safety risks related to medicines. It currently contains more than four million records. The inspection served to verify facts and practices about EudraVigilance.

Regarding CCTV, the inspection aimed to verify compliance with the EDPS video surveillance guidelines, similar to the targeted CCTV inspections carried out in Brussels in 2012, also taking into account the heavy reliance on CCTV in the host Member State.

EMA cooperated fully and constructively with our inspection team. At the time of writing, the inspection report was being finalised.

Targeted CCTV inspection

In February 2012, further to our 2010 Video-surveillance Guidelines, we published a follow-up report which outlined the level of compliance by EU institutions and bodies with EDPS recommendations. The report announced several follow-up measures on the topic, including plans to carry out a number of thematic inspections.



Having conducted inspections on the premises of thirteen Brussels-based EU institutions and bodies between June and July 2012, the EDPS carried out a similar exercise at four Luxembourg-based EU institutions and bodies on 9 and 10 July 2013.

As with the earlier 2012 exercise, our focus was on how Luxembourg-based EU institutions and bodies inform the general public about video-surveillance, including:

- on the existence, location and content of an on-the-spot notice, for instance, with a pictogramme and some basic written information, highlighting that the area is under surveillance;
- on the availability and the content of a more comprehensive data protection notice briefly summarising why and how video-surveillance is taking place, what the safeguards are and how individuals can exercise their rights;
- on the availability and the content of an online policy on video-surveillance detailing the broader approach of the EU institution or body concerned.

The results of the inspections at the EU institutions and bodies are currently being examined.

OLAF-CIS-MAB-FIDE inspection

In December 2013, we conducted an inspection at the European Anti-Fraud Office (OLAF) in Brussels, targeting several parts of the Anti-Fraud Information System (AFIS), namely the Customs Information System (CIS), the Mutual Assistance Broker (MAB) and the Customs Files Identification Database (FIDE). We also analysed the AFIS security framework.

These systems support cooperation between the member states' customs authorities and between them and OLAF, MAB and CIS contain information on seizures of smuggled goods and suspicions of smuggling and other breaches of customs and agricultural legislation. FIDE is an index of persons and entities under investigation and those who have been convicted of customs offences.

The minutes and the report for the inspection are in preparation.

Fact-finding visits

In January and May 2013, we also carried out two fact-finding visits at OLAF in the context of two different complaint cases.

2.6. Consultations on administrative measures

2.6.1. Consultations under Articles 28.1 and 46(d)

On 23 November 2012, we adopted a policy on consultations in the field of supervision and enforcement. The aim of this paper is to provide guidance to EU institutions and bodies and DPOs on consultations to the EDPS based on Articles 28(1) and/or 46(d) of the Regulation.

Article 28(1) of the Regulation stipulates that EU institutions and bodies shall inform the EDPS when drawing up administrative measures which relate to the processing of personal information. Furthermore, Article 46(d) of the Regulation imposes a

duty upon the EDPS to advise EU institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal information.

When an EU institution or body draws up measures affecting data protection rights, it should ensure that proper attention is paid to respecting its obligations under the Regulation before the measure is adopted. One of the most effective means of ensuring this is to involve the DPO at the outset to seek their expert, internal advice.

As outlined in the policy paper, we encourage controllers to submit consultations to us in specific, limited cases when the matter presents: (a) a certain novelty or complexity where the DPO or the institution has a genuine doubt, or (b) a clear impact on data subjects' rights, either due to the risks posed by the processing activities, or due to the scope of the measure.

In principle, the EDPS will only consider consultations which have first been submitted for consultation to the DPO of the institution concerned (Article 24.3 of the Rules of Procedure). In 2013, we received 37 consultations on administrative measures.Within the framework of consultations on administrative measures envisaged by an institution or body, a variety of issues were examined in 2013, some of which are reported below.

2.6.1.1. Transfer of staff data to member states' Permanent Representations

The DPO of an EU Agency consulted the EDPS on the transfer of personal data of staff members to the Permanent Representations of member states. The main responsibility of Permanent Representatives is to collectively prepare the work of the Council of the European Union as part of the COREPER committee.

In our reply of 9 April 2013, we pointed out that such requests should always specify a purpose and be subject to a clear legal basis, for instance Article 15, second subparagraph of Protocol No. 7 to the Treaty on the Functioning of the European Union (TFEU) on the privileges and immunities of the EU, providing that the names, grades and addresses of officials and other staff in certain categories "shall be communicated periodically to the governments of the Member States".

2.6.1.2. Change of purpose for the use of data collected for a specific purpose

On 17 April 2013, we replied to a consultation from an EU body, which asked about the legality of using personal information collected from an access security or time management system for another purpose, more specifically in order to instruct a disciplinary procedure in an investigation.

In our answer, we conducted an analysis based on the purpose limitation principle (Article 4) and change of purpose (Article 6).

We concluded that the rules governing disciplinary procedures and fraud investigations permit the use of any relevant types of data in the context of disciplinary investigations. Furthermore, we considered that the processing of the data stemming from the access security or time management system can be considered compatible in the framework of disciplinary proceedings.

However, the authorisation must be strictly interpreted, so that the proportionality and necessity of the processing is respected and that re-use for another purpose is only permitted in the specific context of an open disciplinary process for a specific case. Similar issues have been dealt with in the context of prior checks (see section 2.3.3.1).

2.6.1.3. Public access requests at the ECB - balancing the interests of staff and the public

On 20 September 2013, we replied to a consultation from the European Central Bank (ECB) about public access to a register set up as part of the ethical framework rules of the ECB on the gifts received by ECB staff members.

Taking into account the ECB decision on public access and the facts of the case, our analysis built on the CJEU's Bavarian Lager judgment and the EDPS Paper on Public access to documents containing personal data after the Bavarian Lager ruling and considered the public access request as a transfer that must be compliant with Regulation 45/2001. The ECB must balance the interests of the recipient to establish the necessity of the transfer of information and that of the institution to establish if there is reason to assume that an individual's legitimate interests might be prejudiced by allowing access to his personal information.

The balance of interests should also take into account the categories of staff concerned as transparency requirements may justify the publication of personal data of executive members or senior management members.

We concluded that the ECB should assess the possible public nature of the gift register and make clear to the persons mentioned in the register to which extent the processing might be publicly disclosed. Consequently, an individual would need to be informed before his personal data is disclosed for the first time and should have the right to object to the disclosure on compelling legitimate grounds pursuant to the Data Protection Regulation.

2.7. Data protection guidance

The experience gathered in the application of the Data Protection Regulation has enabled us to translate our expertise into specific guidance for institutions and bodies. In 2013, this took the form of guidance in the areas of public procurement, grants and external experts, as well as follow-up to previous guidance to institutions in the areas of leave and flexitime, training for DPOs, workshops for controllers and DPOs, a dedicated area for DPOs on the EDPS website and a telephone helpline for DPOs.

2.7.1. Thematic Guidelines

In the spirit of the action plan established in the Strategic Review 2013-14, and on request from stakeholders for more guidance in the area of data protection, we continued our work on developing thematic Guidelines. These not only cover areas

subject to prior checking by the EDPS but also more horizontal themes.

Where our Guidelines cover areas that are subject to prior checks by the EDPS, they have contributed to reducing this work and have allowed us to focus our Opinions on processing operations that diverge from the Guidelines.

- Guidelines on Public Procurement, Grants and External Experts

In June 2013, we published Guidelines on the processing of personal information in the context of public procurement, grants, selection and use of external experts. All these procedures are based on the EU Financial Regulation and involve evaluation of the respective applicants according to the same set of criteria. The main issue raised in the Guidelines was the conservation of personal data in this context. We highlighted the respective provisions of the Rules of Application for the EU Financial Regulation, allowing for conservation of data for control and audit purposes for up to seven years after the signature of the related contract or agreement.

- Survey on Data Conservation in an Evaluation Context

As a follow up to the 2011 Staff Evaluation Guidelines, we conducted a survey on the conservation of personal information in an evaluation context in June 2013. A questionnaire was sent to the participants of our 2012 Data Conservation Workshop to gather information from HR experts and Document Management Officers on the reasons for the existing time limits as well as the storage on electronic files.

- Guidelines on the processing of personal information in the area of leave and flexitime

At the end of 2012, the EDPS provided guidance to EU institutions and agencies by adopting Guidelines concerning the processing of personal information in the area of leave and flexitime. These Guidelines were designed to offer practical guidance and assistance to all DPOs and controllers in their task of notifying existing and/or future data processing operations in this area to the EDPS.

In 2013, the EDPS received numerous notifications for prior checks from EU institutions and bodies linked to these Guidelines. These notifications allowed us to analyse the implementation of the Guidelines more precisely. Instead of adopting a general Opinion covering all the notifications received, we adopted specific Opinions covering leave and flexitime processing operations in general per each agency, and we focused our analysis on the aspects of the processing operations that diverged from the Guidelines.

2.7.2. Training and workshops

On 31 January 2013, special training was organised for the DPOs of five EU Joint Undertakings, ARTEMIS, Clean-Sky, ENIAC, IMI & SESAR. Presentations focused on the role and missions of the DPO, the guidance available on the EDPS website (specifically, the DPO corner), EDPS compliance monitoring tools and EDPS enforcement powers.

On 25 February 2013, upon a specific request from the European Training Foundation (ETF), the EDPS organised a thematic training session for the agency staff dealing with HR, IT and public procurement matters. Most of the participants confirmed that they gained new insight, on the practical

implementation of the EDPS Guidelines in these fields and that the training was a useful exchange of views with EDPS staff. It is interesting to note that some of the participants identified the importance of the prior notification process, that prior checking is an opportunity and that they should check the EDPS website for guidance and Opinions when drafting policies and procedures.

On 10 April 2013, we organised a training session upon a request from the DPO of the European Defence Agency (EDA) for various controllers in the agency. The EDPS staff focused on the importance of submitting notifications to the DPO, on how controllers should fill in notifications and provided concrete examples on data subjects' rights. The training proved to be useful, since it raised awareness and motivated the controllers to submit their notifications to the agency's DPO, who then sent them to the EDPS for prior checking.

On 17 April 2013, we organised a general training for DPOs from EU institutions & bodies with a focus on the prior check procedure. Presentations were given on the duties of the DPO in this area, the steps involved in the prior check procedure, applicable deadlines, as well as the guidance available on the EDPS website. The training included a group exercise to complete an actual notification form for prior checking.

We also launched a series of workshops that will help us to issue guidance on technology-related subjects. The discussions in the workshops confirm the need for a common approach in protecting personal information and highlight the benefits of EU institutions and bodies exchanging experiences on good data protection practice, particularly in such complex and rapidly developing technological fields.

The first in this series was a workshop held on 12 June 2013 on the use of electronic communication in the workplace. 75 participants, including DPOs, DPCs and staff from the IT and HR fields, represented the majority of EU institutions and bodies. They offered valuable contributions from their day-to-day work on the use of phones, internet and email. Other meetings and email contact with DPO/DPC networks, IT, HR and staff from other fields within the EU administration will help to gather other pertinent information with a view of drafting guidance in this area.

On 19 September 2013, we held two workshops on the use of mobile devices in the workplace and on websites managed by EU institutions and bodies. Over 60 participants attended each workshop. Prior to the meeting, we asked those that had registered for the workshop to take part in our survey on their own practices. This gave us a unique and valuable insight into the experience and views on the issues that were subsequently debated, including the use of website cookies and private mobile devices in the workplace.

Transfers workshop

A workshop on trans-border data flows for DPOs was organised on 22 November 2013. The aims of the workshop were twofold, to address the main lines of the legal regime, as established in Article 9 of Regulation 45/2001 and as a forum within which to discuss the experience of DPOs in the field: cases, needs and problems encountered. The event began with a presentation that addressed the *notion* of transfers, the scope of Article 9, the principle of *adequate protection*, derogations, adequate safeguards, legislation and bilateral agreements, and supervision and enforcement in the field of transfers. The workshop was very well attended and a fruitful exchange of ideas took place.

2.7.3. DPO Corner and other tools

The DPO corner of the EDPS website is a restricted section reserved for the DPOs of EU institutions

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

We also set up a telephone 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)[6].

6 We usually receive approximately ten of such queries per month.

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.

Our guiding principles

- we seek to engage constructively with policy makers at an early stage of policy development;
- we seek creative solutions that support policy goals and the principles of personal privacy, drawing on our knowledge of law and technology;
- we work to find practical solutions, particularly in complex policy areas, which may require difficult balances to be struck and difficult judgments to be made;
- we seek to ensure that data protection will be an integral part of policy-making and legislation, in all areas where the EU has competence.

3.1. Introduction: overview of the year and main trends

2013 continued to be a year of major developments in the field of data protection, two of which had a significant influence on our work.

The debate following the Edward Snowden revelations shed light on the methods of mass surveillance in the EU and the USA. The revelations did much to raise awareness about privacy and data protection among the general public and were an opportunity for us to offer guidance to the EU legislator and other interested parties. In his speech, at the European Parliament´s Civil Liberties (LIBE) Committee public hearing on the electronic mass surveillance of EU citizens in October 2013, the EDPS insisted that it is time to reclaim control of our privacy in the EU. In November 2013, the Commission consulted us on its communication *on Rebuilding trust in EU-US data flows*. We have already provided informal comments, but will present a formal Opinion on the subject in early 2014.

The reform of the existing data protection rules in the EU was the other dominant theme of the year. This project featured high on our agenda in 2013 and will remain there as the legislative procedure continues. The on-going discussions in the European Parliament and the Council have generated enormous interest from the public and private sectors, both from within and outside the EU. The process has also demonstrated a fundamental understanding of the underlying principles of the reform by the EU institutions. On 15 March 2013, we sent our additional comments on the reform to the European Parliament, the Commission and the Council. We also continued to be involved in the discussions in the Parliament and Council.

Notwithstanding these issues and following the trend of past years, the areas covered by our Opinions continue to diversify. In 2013, the Commission published a large number of legislative proposals affecting the fundamental right to the protection of personal data. Aside from our traditional priorities, such as the further development of the Area of

Freedom, Security and Justice (AFSJ) or international data transfers, new fields are emerging, such as the Digital Agenda and the internet as well as financial issues and eHealth.

The Digital Agenda and the internet were addressed in our Opinion on the Commission communication on the Digital Agenda for Europe – Driving European growth digitally, our Opinion on the European Single Market for electronic communications and the Opinion on a green paper entitled Preparing for a fully converged audio-visual world: Growth, Creation and Values.

In the AFSJ, we published Opinions on Europol, the EU cyber security strategy and smart borders as well as on EU-Canada PNR and the European Information Exchange Model.

As for the internal market, we published Opinions on anti-money laundering and terrorist financing, payments in the internal market, European company law and corporate governance and electronic invoicing in public procurement.

In the area of eHealth, our Opinions on medical devices, drug precursors and the eHealth action plan were highlights.

3.2. Policy framework and priorities

3.2.1. Implementation of consultation policy

Although our working methods in the area of consultation have developed over the years, our basic approach to interventions has not changed. Our policy paper of March 2005 *The EDPS as an advisor to the Community institutions on proposals for legislation* and related documents remains relevant, although it must now be read in light of the Lisbon Treaty.

Based on Articles 28(2) or 41 of Regulation (EC) No 45/2001, formal Opinions are our main instruments in consultation work, containing a full analysis of all the data protection related elements of a Commission proposal or other relevant instrument.

Legislative consultations based on Article 28(2) of the Regulation are a core element of the EDPS' advisory role. According to this article, the Commission shall consult us when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms. Our Opinions fully analyse the data protection implications of a proposal or other text.

As a rule, we only issue Opinions on non-legislative texts (such as Commission working documents, communications or recommendations) if there are significant data protection implications. Occasionally, written comments are issued for more limited purposes, so as to quickly convey a fundamental political message or to focus on one or more technical aspects. They are also used to summarise or repeat observations made earlier.

We are available to the EU institutions for advice throughout all the phases of policy making and legislation and we use a wide range of other instruments in our advisory role. Although this requires close contact with the institutions, maintaining our independence remains paramount.

Other instruments include presentations, explanatory letters, press conferences or press releases. For instance, Opinions are often followed by presentations in the Committee for Civil Liberties, Justice and Home Affairs (LIBE) or other committees of the European Parliament or in the relevant working parties of the Council.

A recent addition to these instruments is the publication of forward looking guidelines and preliminary Opinions. Through these publications we aim to explain the importance and benefits of proper implementation of data protection principles. They will be prepared on our own initiative and not linked to a specific legal proposal, with the intention of providing policy makers and regulators with a benchmark for the application of fundamental principles in future policy making.

Consultations with the Commission take place at various stages in the preparation of their proposals and frequency varies depending on the subject and on the approach followed by the Commission services.

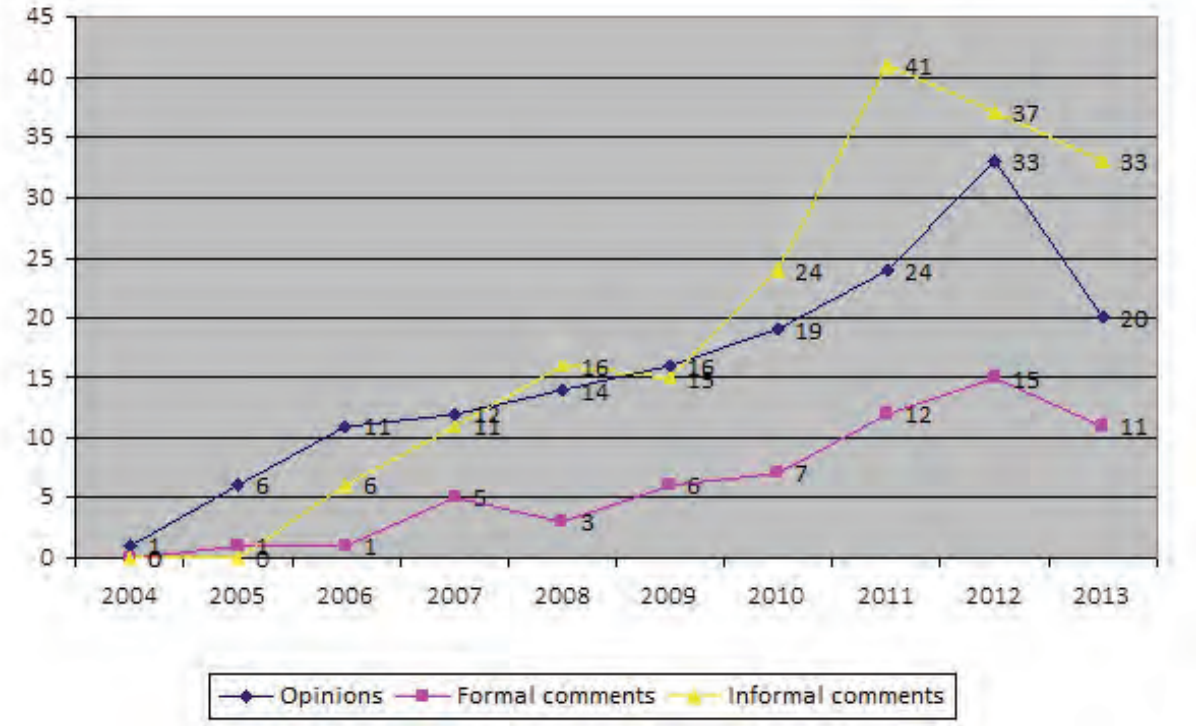
Formal consultations are quite often preceded by a request for informal comments. When the Commission drafts a new legislative measure with an impact on data protection, the draft is normally sent to us during the inter-service consultation stage, i.e. before the proposal is finalised and adopted. These informal comments, of which there were 33 in 2013, allow data protection issues to be addressed at an early stage when the text of a proposal can still be changed relatively easily. The sub-

mission of informal comments to the Commission is a valuable way of ensuring due consideration for data protection principles at the drafting stage of a legislative proposal and critical issues can very often be resolved at this stage. As a rule, these informal comments are not public. If they are followed by an Opinion or formal comments, we will usually refer to the informal comments that we submitted earlier.

Regular contact with the relevant services of an institution will take place following the issuing of our comments or Opinion. In some cases, we are heavily involved in the discussions and negotiations taking place in Parliament and Council. In others, the Commission is the main interlocutor in the follow-up phase.

3.2.2. Results of 2013

In 2013, there was a slight decrease in the number of Opinions we issued compared to the steady increase of previous years. To a large extent, this is the result of a successful focus on strategic priorities, including the review of the data protection framework. The EDPS issued 20 Opinions, 13 formal comments and 33 informal comments on a variety of subjects. With these Opinions and other instruments used for intervention, we implemented the EDPS priorities for 2013, as laid down in our Inventory.



3.3. Review of the EU Data Protection Framework

Following our many activities on the reform in 2012 and our Opinion of March 2012, we sent additional comments to the European Parliament, the Commission and the Council on 15 March 2013. Our comments related to specific areas that needed clarification and also reacted to the amendments proposed by the relevant committees of the European Parliament.

In our comments, we reiterated that pseudonymised data remains personal data (or personal information) and should be protected as such. Any definition of anonymous data or pseudonymous data should, therefore, be fully consistent with the definition of personal data and should not lead unduly to the removal of certain categories of personal data from the scope of the data protection framework. We also advised against excluding specific sectors from the scope of application of the EU data protection frame-

work and against limiting the territorial scope of the proposed general data protection Regulation.

We supported the elimination of the potential further processing of data for incompatible purposes and stressed that the definition of explicit consent should be maintained. We also supported the definition and responsibilities of controllers and processors as proposed by the Commission, as well as the principle of accountability, which should apply to the whole package. Some of the elements of the so called risk-based approach were welcome but we pointed out that full protection as provided for in the Regulation should apply to all processing operations. As regards international transfers, we recommended that the rules be clarified and welcomed the amendments introducing a new article on transfers not authorised under EU law.

As regards the proposed data protection Directive on criminal law enforcement, we supported the closer alignment of the proposed Directive with the proposed Regulation to ensure consistency. We also welcomed the amendments introducing specific conditions and safeguards for access by law enforcement authorities to data initially processed for other purposes and highlighted that any transfer to non-law enforcement authorities or private parties should be strictly limited.

Following tough negotiations and many political compromises, the LIBE Committee of the European Parliament voted in support of its report on 21 October 2013. Important progress has been made, but the political process within the Parliament is not yet complete as the next and final step in the Parliament's first reading is a plenary vote.

In Council, less progress has been made. Negotiations between member states on important parts of the legislative framework such as the one-stop-shop mechanism and the approach of a package containing a Regulation and a Directive, among other politically sensitive and legally complicated issues, are continuing.

In the course of 2013, we continued to give advice to the European Parliament and the Council and contributed to the debate. We also contributed to the beginning of the process of revision of Regulation (EC) No 45/2001, which governs data processing carried out by the European institutions, by sending a letter to the Commission outlining our initial views.

3.4. Area of Freedom, Security and Justice and international cooperation

3.4.1. Strengthening law enforcement cooperation in the EU: the European Information Exchange Model

On 29 April 2013, we adopted an Opinion on the Commission communication *Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)*. We appreciated the general attention devoted to data protection in the communication and were pleased that the communication concludes that neither new EU-level law enforcement databases nor new EU information exchange instruments are needed.

However, we emphasised the need for a full evaluation process of the existing instruments and initiatives in the Justice and Home Affairs area, the outcome of which should lead to a comprehensive, integrated and well-structured EU policy on information and exchange management.

3.4.2. Europol

On 31 May 2013, we adopted an Opinion on the Commission proposal for a new legal framework for the EU Agency for Law Enforcement and Training (Europol). In our Opinion we stressed that the proposal has significant implications for data protection since the processing of information including personal data is the principal reason for the existence of Europol. We also emphasised that a strong framework of data protection is important not only for data subjects, but also contributes to the success of police and judicial cooperation.

We understood the need for innovative and flexible approaches in preventing and combating serious crimes, but also insisted on strong safeguards

and the necessity to clearly define the purposes of the data processing carried out by Europol as well as the criteria for data transfers to third countries and international organisations. We also made recommendations to further improve the data protection regime of Europol and in particular welcomed the strong architecture for supervision on data processing, which includes supervision by the EDPS and, where relevant, with the active involvement of national DPAs.

In letters to the Council and the Parliament in November 2013, we further explained the need for the strong supervision of Europol.

3.4.3. EU Cyber security strategy

On 17 June 2013, we published an Opinion on the EU's strategy on cyber security. We emphasised that if cyber security is to contribute to the protection of personal data in the online environment, it cannot be an excuse for the unlimited monitoring and analysis of the personal information of individuals. While there is a welcome acknowledgement of the importance of data protection principles when managing security in cyberspace, the strategy is not clear on how these principles will be applied in practice.

We observed a lack of clarity as to the integration of proposed measures with existing and forthcoming data protection and security legislation. We noted that the role of data protection authorities in the implementation and enforcement of security obligations and in enhancing cyber security was not properly considered. In addition, the exchange of security information among competent national security authorities as set up by the proposal does not yet provide guarantees for adequate security levels and for the protection of personal data.

3.4.4. Smart borders

On 18 July 2013, we issued our Opinion on smart borders, which focused specifically on the Entry/Exit System. In our Opinion, we stated that there is no clear evidence that the Commission proposals to create a smart border system for the external borders of the EU will fulfil the aims that it has set out. We considered that one of the stated aims of the proposals was to replace the existing "slow and unreliable" system, but the Commission's own

assessments do not indicate that the alternative will be sufficiently efficient to justify the expense and intrusions into privacy.

We agreed that improving the management of border controls is a legitimate exercise. However, we commented that it would be more effective to do this once a clear European policy on the management of over stayers has been established. In the absence of such a policy, the creation of yet another large-scale IT database to store massive amounts of personal information is a disproportionate response to a problem that other recently created systems may be able to help solve. It would be prudent both economically and practically to evaluate existing systems, at least to ensure consistency and best practise.

3.4.5. EU-Canada PNR

On 30 September 2013, we issued our Opinion on the Commission proposals on the conclusion and the signature of the agreement between Canada and the EU on the transfer and processing of Passenger Name Records (PNR).

As in our previous Opinions on EU PNR agreements, we questioned the necessity and proportionality of PNR schemes and the bulk transfers of PNR data to third countries. We also questioned the choice of the legal basis, which in our view should primarily be Article 16 of the TFEU concerning the protection of personal data, rather than Article 82(1)(d) and Article 87(2)(a) on judicial cooperation in criminal matters and police cooperation.

We also expressed concerns about the limited availability of independent administrative redress and full judicial redress for EU citizens not present in Canada and questioned the appropriateness of an executive agreement to achieve them. We also recommended that it be made clear that no other Canadian authority can directly access or request PNR data from carriers.

3.5. Internal Market including financial data

3.5.1. European company law and corporate governance

In its *Action plan on European company law and corporate governance: balancing investor privacy and the need for regulatory oversight and transparency*, the Commission outlined its initiatives to modernise the company law and corporate governance framework in Europe.

In our letter of 27 March 2013, we reminded the Commission that any legislative proposals aimed at increasing the visibility of shareholdings must take due account of shareholders' rights to protect their personal information. Policy makers need to carefully assess and clearly articulate the public policy objectives that increase this visibility and balance them against the risks to shareholders' rights to protect their privacy.

Better shareholder oversight of remuneration policy is another area in the proposal where transparency needs to be balanced with the rights of individuals to their privacy and protection of their data. We encourage the exploration of different methods, modalities and granularities of making personal data publicly available to ensure that the measures adopted are proportionate for any scenario that allows access to information on the remuneration of individual members of management and/or supervisory boards to the public.

3.5.2. Regulation on the market surveillance of products

In our Opinion of 30 May 2013, we analysed the Commission's proposed Regulation on the market surveillance of products which aims to ensure that products do not endanger health, safety or any

other aspect of public interest and that they comply with the requirements set out in the EU product harmonisation legislation. In the Opinion, we stressed that a proposal should always consider whether EU data protection rules are applicable, especially where the sharing of information is allowed for, whether through dedicated IT platforms or not.

As a rule, whenever a legislative proposal involves the processing of personal information, even if it is not the main purpose, national rules implementing the Data Protection Directive 95/46/EC or the provisions of Regulation (EC) No 45/2001 are applicable. Certain conditions apply, therefore, whenever personal information is to be collected, analysed or processed. For example, only personal information that is strictly necessary for the stated purpose should be collected and specific time-limits for the retention of the information collected should be set.

We also highlighted that where the personal information of an economic operator (e.g. the manufacturer, their authorised representative, the importer and/or the distributor of a product available on the EU market) is to be made public, the kind of personal data that is to be published and the reasons for doing so must be made explicit in an advance privacy notice to those concerned.

3.5.3. Payment account fees

On 27 June 2013, we issued formal comments on the Commission proposal for a Directive on the comparability of fees relating to payment accounts, payment account switching and access to payment accounts with basic features. The proposal outlines the measures for the comparability of payment account fees, giving consumers an overview of the offers on the market and the measures for switching which would make it easy for them to change their account if a better offer is available. All these elements aim to reinforce competition in the financial services market to the benefit of consumers. However, to guarantee that as many consumers as possible can really enjoy the benefits of these improvements, it is essential to ensure that every EU citizen has the right of access to basic payment account services.

We were pleased that any exchange of consumer personal data by payment service providers in the 'switching phase' is subject to the prior written and explicit consent of the consumer. We also welcomed that the proposed Directive specifically recalls the principle of necessity in information sharing among payment service providers. However, we stressed that the proposal should mention that relevant EU data protection legislation remains fully applicable in relation to the obligations introduced by the Directive.

3.5.4. Anti-money laundering

On 4 July 2013, we issued an Opinion on the Commission proposals for a Directive preventing the use of the financial system for the purpose of money laundering and terrorist financing and for a Regulation on the information on the payer that accompanies the transfer of funds. We acknowledged the legitimacy of achieving transparency of payments sources, fund deposits and transfers in order to fight terrorism and money laundering but insisted that data protection requirements should be included in legislation transposing international standards at EU level. We regretted that neither the proposed Directive nor the Regulation fully addressed data protection concerns and did not clarify the application of EU data protection rules to the specific processing activities involved. In the proposed texts no substantive provision addressed data protection issues.

More specifically, we expressed concerns about the large amounts of personal information collected in the name of anti-money laundering and anti-terrorist purposes, in particular by professionals carrying out customer due diligence. We recommended that the purpose limitation principle be strictly respected and that further guidance be given to professionals on the data that they should or should not collect. We also highlighted that the texts should further develop the role of the rights of individuals and in particular, raise the awareness of professionals and customers. We also advised that limiting the rights of individuals is justified only if it is proved necessary.

Considering the repeated, mass and structural transfer of personal data that will take place in the framework of the proposed Directive and Regulation, we highlighted the risks linked to such trans-

fers to third countries and advised the inclusion of dedicated substantive provisions on the transfers of personal data, such as a proportionality test, to ensure proper protection of individuals when their information is transferred.

In addition we pointed out that the data retention periods chosen need to be justified. We also insisted that the publication of sanctions imposed on professionals that do not respect their obligations under these texts, need to comply with the proportionality principle.

3.5.5. Sale of counterfeit goods via the Internet

On 11 July 2013, we published our comments on the Commission report on the functioning of the memorandum of understanding (MoU) on the sale of counterfeit goods via the internet. We welcomed the publication of this report, which provides information on how internet platforms in the MoU have implemented notice and take down procedures and on the mechanisms they have set up for cooperating and sharing information - including the personal information of alleged infringers - with rights owners.

We noted the Commission's role in recognising the importance of these issues and facilitating dialogue between companies and trade associations to ensure that any measures deployed are compliant with the applicable law and fully respect the rights of individuals to privacy and data protection. We also expressed a wish to be involved in the on-going dialogue.

3.5.6. Trade mark protection

On 11 July 2013, we issued an Opinion on the Commission proposals for a Directive to approximate the laws of the member states relating to trademarks and a Regulation amending the Community trade mark regulation. In our Opinion, we stressed that the collection and processing of personal data by the central industrial property offices in the member states and the European Internal Market Office (OHIM) must comply with the applicable data protection law.

We also recommended that the modalities for the exchanges of information through common or connected trade mark databases and portals be clearly established, in particular by determining the authorised recipients of personal data, the types of data, the purpose of such exchanges and the length

of the retention of the data in those IT systems. Furthermore, we recommended that if the exchanges of information between OHIM and national offices include personal data then this, as well as the types, should be clarified.

3.5.7. Electronic invoicing in public procurement

On 11 November 2013, we issued an Opinion on a Commission proposal for a Directive on electronic invoicing in public procurement. In the Opinion, we supported the objective of the Commission to facilitate the move towards paperless eInvoicing. At the same time, we drew attention to the privacy and data protection risks that will be increased as a result of the increased availability of invoice data in paperless and machine-readable form for further purposes.

While we acknowledged that permissible further uses of data may exist, for example, in the context of ePayments and eArchiving; we warned that other purposes, such as automated profiling and data-mining for tax and law enforcement purposes will likely not be considered as compatible and may only be possible, if at all, subject to the exceptions and strict criteria of Article 13 of Directive 95/46/EC.

3.5.8. Payments in the Internal Market

On 5 December 2013, we issued an Opinion on the proposed Directive for payment services in the internal market. In our Opinion, we welcomed the introduction of a substantive provision that stated that any processing of personal data taking place in the framework of the proposed Directive should be done with full respect to the national laws implementing Directive 95/46/EC and Directive 2002/58/EC and of Regulation EC No 45/2001.

We recommended that references to applicable data protection law should be specified with concrete safeguards that will apply to any situation in which personal data processing is envisaged and it should be expressly clarified that the processing of personal information may be carried out insofar as is necessary for the performance of payment services. We also highlighted other data protection issues, for example, in the exchanges of information, third party access to account information and security reporting.

3.6. Digital Agenda and technology

3.6.1. Radio equipment

The Commission proposal for a Directive harmonising the laws of member states that relate to the availability of radio equipment on the market will replace Directive 1999/5/EC on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (the so-called R&TTE Directive).

With some exceptions, any equipment that makes use of radio waves or telecommunication frequencies would fall within the scope of these rules, for example, cars equipped with SIM cards (such as the integrated eCall discussed in section 3.9.3.), which make use of radio equipment. As the use of such technology allows for the tracking of the location of a vehicle (and thereby of a person), its use has implications for the privacy of individuals. In our formal comments of 27 February 2013, we noted that the R&TTE Directive incentivised manufacturers of such equipment to apply privacy by design.

We were therefore pleased that the proposal builds on the approach of the R&TTE Directive in privacy and data protection terms as they remain essential requirements for the design of radio equipment. We also welcomed that the proposal clearly imposes responsibility on manufacturers for ensuring that radio equipment placed on the market has been designed and manufactured so that it incorporates, among other things, safeguards to ensure the protection of personal data and privacy of consumers. However, we regretted that fixed terminal equipment has been removed from the scope of the Directive, which reduces the incentive for building privacy by design in such equipment. This is particularly regrettable since terminal equipment plays an increasingly important role for the protection of privacy and there is no equivalent rule on the protection of personal data and privacy in other legislative instruments that apply to terminal equipment not using radio.

We therefore recommended that the proposal include a commitment from the Commission to monitor the compliance of terminal equipment with data protection and privacy requirements and to consider appropriate measure should the need arise.

3.6.2. The Digital Agenda for Europe - Driving European growth digitally

In its Communication on *The Digital Agenda for Europe - Driving European growth digitally*, the Commission has identified various policy areas on which it will focus its efforts to enable and stimulate the development of the digital economy, such as the Digital Single Market, very fast internet supply and demand, cloud computing and trust and security.

In our Opinion of 10 April 2013, we emphasised that any design and deployment of new information communication technology (ICT) applications and solutions for the digital environment must respect data protection principles, especially since the principle of *privacy by design* will become a legal obligation under the proposed data protection Regulation. We also reminded the Commission that there should be an appropriate legal basis for the use of interoperability as a means to facilitate data sharing among databases, together with appropriate data protection safeguards.

In the area of cloud computing, we referred to the extensive guidance on the application of current data protection law and on the impact of the proposed data protection Regulation that has been provided by data protection authorities as well as the EDPS. We urged the Commission to act upon this guidance to help foster the trust of individuals and customers in these new technologies, which in turn will ensure their successful deployment.

3.6.3. Preparing for a Fully Converged Audio visual World: Growth, Creation and Values

On 24 April 2013, the Commission published a Green Paper entitled *Preparing for a Fully Converged Audio visual World: Growth, Creation and Values*. The Green Paper launched a public consultation on the implications of the on-going transformation of the audio visual media landscape: audio-visual media services are no longer only provided by traditional means and by traditional broadcasters but are also delivered by providers on demand via the internet and reach consumers through connected (often called 'smart') TVs, PCs, laptops or tablets and mobile devices such as smartphones.

In our comments of 30 August 2013, we stressed that these new modes of distribution and consumption of audio visual works generate new forms of collection and processing of users' personal information. However, it may not always be clear for users that their consumption of audio visual works and interaction with associated services leads to the processing of personal data at different levels of the provision of the services (for instance, by their device, by their ISP and/or broadcaster) nor to what extent such processing takes place, in such a way that users are not in control of their information.

We believe that any policy choice in that area should be fully compliant with the EU data protection legal framework. Among other things, we highlighted that full transparency must be ensured to users on the types of personal data collected about them and by whom, consent of the user to the processing of their data should be sought where relevant and specific attention should be paid to the protection of the privacy and personal data of children, especially in the field of advertising. Technical tools should help protect children's privacy and personal data.

3.6.4. European Single Market for electronic communications

On 14 November 2013, we published an Opinion on the Commission proposal for a Regulation harmonising electronic communications services across the EU.

In our Opinion, we cautioned that the proposed measures would unduly limit internet freedom. We welcomed the inclusion of the principle of net neutrality - the impartial transmission of information on the internet – in the text, but also said that it is devoid of substance because of the almost unlimited right of providers to manage internet traffic. We also warned against the use of highly privacy intrusive measures under the broad umbrella of crime prevention or to filter content illegal under national or EU law, as incompatible with the principle of an open internet.

Confidence in our digital environment in the years ahead depends on our capacity to provide legal and technical infrastructures that can generate and preserve trust in the Digital Society. This confidence has already been seriously undermined by the various surveillance scandals recently. To re-build consumer confidence in the electronic communications market in the EU, users need to be certain that their rights to privacy, confidentiality of their communications and protection of their personal information are respected. We urged the Commission to outline more precise reasons for which traffic management measures can be applied. Any interference with their rights must be clearly communicated to users, allowing them to switch to those providers that apply less privacy-invasive traffic management techniques in their services.

Finally, we noted that the supervision of any application of traffic management measures by providers should include a greater role for national data protection authorities to ensure that the privacy and data protection rights of users are fully respected.

3.7. Public health and consumer affairs

3.7.1. Drug precursors and third countries

On 18 January 2013, we published an Opinion on the Commission proposals for amending the regulations on intra-EU trade and on trade with third countries on drug precursors (legal substances used in the illicit manufacture of narcotics and psychotronic substances). We welcomed the references in the proposals to the applicability of EU data protection legislation, that many of the categories of information to be processed were specified and that the principle of purpose limitation was mentioned in the external trade proposal.

However, we recommended that the main legislative texts outline all essential elements of the processing operations, such as the exclusion of the processing of sensitive data. In addition, all the categories of information to be processed should be specified at the very least by delegated acts but preferably also in the proposals.

Among our other recommendations were that the intra-EU trade proposal should specify that personal information on suspicious transactions may only be used for the purpose of preventing the diversion of scheduled substances, that maximum retention periods for all processing operations should be laid down, and that appropriate safeguards for international transfers of personal information should be provided.

Furthermore, we recommended that clarification on who has access to the new European database on drug precursors is provided and that the coordinated supervision of the European database by the EDPS and national data protection authorities, similar to the supervision for the Internal Market Information System, is ensured. We also recommended prohibiting the interconnection of the European database with other databases created for different purposes.

3.7.2. Medical devices

The proposed Commission regulations on medical devices and in-vitro medical devices will imply the processing and storage of large amounts of personal information, potentially saving sensitive data such as patient health information in a European central database (Eudamed).

In our Opinion of 8 February 2013, we recognised and welcomed the specific attention paid to data protection in the proposed regulations. However, we see the need for further improvement and clarification, for example, on the types of categories of personal information to be processed, particularly where sensitive health data might be processed and stored. We recommended that the proposed regulations specify the circumstances under which personal health data may be included in the Eudamed database and that the safeguards for such processing and storage also be outlined.

3.7.3. eHealth Action Plan

In our Opinion of 27 March 2013, on the Commission communication for an *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century,* we welcomed the attention paid to data protection in the communication. However, the personal information processed in the context of eHealth and well-being through information communication technology (ICT) applications and solutions, often relates to health data, which requires a higher level of data protection.

We urged industry, member states and the Commission to carefully consider the data protection implications when implementing initiatives within the eHealth area. Furthermore, we recommended that the Commission consult the EDPS before it takes further legislative and non-legislative action as described in the Communication.

3.7.4. Drug precursors and Russia

On 23 April 2013, we adopted an Opinion on the Commission proposal for the conclusion of an agreement between the EU and the Russian Federation on drug precursors. The aim of the agreement is to increase cooperation to prevent legal substances from being used for the illicit manufacture of narcotics and psychotropic substances (called drug precursors). The agreement will, for instance, allow the transfer of personal information on suspected transactions of drug precursors.

We welcomed the provisions on personal data protection in the text of the agreement and the inclusion of mandatory data protection principles in the annex. However, we were concerned about the actual enforceability of these principles, so we recommended that EU and Russian data protection authorities jointly review the implementation of the agreement. We also recommended that the text provide explicitly for the possible suspension or termination of the agreement if data protection principles are breached.

In addition, we advised better specification of data protection safeguards, for example the purpose of the transfers of personal information, the retention periods, the categories of data to be exchanged and the protection of data relating to suspect transactions. In the interests of completeness of the mandatory data protection principles, we recommended adding provisions relating to sensitive data, data security and the restriction of the onward transfers of personal information.

3.7.5. Prices of medicinal products for human use

On 30 May 2013, we adopted an Opinion on the amended Commission proposal for a Directive on

the *transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of public health insurance systems*. The aim of the proposal is to ensure that national rules on pricing and reimbursement of medicines do not oppose the principle of the free movement of goods in the EU.

We emphasised that personal information processed in the context of the pricing and reimbursement procedures of national health authorities may relate to patient health data. As a consequence, a higher level of data protection is required. We recommended that any patient health data included by a pharmaceutical company in its submission for authorisation to put a medicinal product on the market is fully anonymised - in other words, that the identity of the person cannot be determined - before this data is transferred to the national health authorities for any further processing. We also questioned the necessity and proportionality of the mandatory publication of names and declarations of interest of experts, members of decision making bodies and members of bodies responsible for remedy procedures.

3.8. Publication of personal information

3.8.1. Insolvency proceedings Regulation

On 27 March 2013, we adopted an Opinion on the Commission proposal for a Regulation on insolvency proceedings. We welcomed the references that the Proposal made to the applicability of EU data protection legislation. However, we recommended that the substantive provisions should be clearer on how data protection principles apply concretely to insolvency proceedings, in particular to the information exchanged between stakeholders which is also sometimes published.

We expressed concerns about the publication of information relating to the opening and closing of insolvency proceedings in insolvency registers which are accessible to the public, on the internet, free of charge. We acknowledged that the aim of encouraging transparency and communication between stakeholders is legitimate, yet considered that this particular method of publication raises specific risks and is privacy intrusive.

We pointed out that the proportionality of this measure was not proven since, contrary to the approach laid down in the *Schecke* ruling, no alternative option, i.e. a different method of publication that would cause less interference with the beneficiaries' right to private life, has been considered. Among other things, we advised that data controllers are designated, updates of the data exchanged or published are organised, the retention period of the data processed is specified and that procedures are set up to inform data subjects of the processing of their personal information.

3.9. Transport

3.9.1. Occurrence reporting in civil aviation

An occurrence is any event that could affect aviation safety, including accidents, defects, faults and other problems associated with the operation of aircrafts. To ensure more comprehensive and high quality reporting the proposal outlines, among other things, a voluntary reporting system to supplement the mandatory system and encourages organisations - and not only member states - to report occurrences. The proposal also offers harmonised protection from hierarchical punishment or the prosecution of individuals reporting occurrences and aims to ensure adequate access to information contained in the European Central Repository.

In our Opinion of 10 April 2013 on the Commission proposal for a Regulation on occurrence reporting in civil aviation, we welcomed the attention paid to the protection of personal data in the proposal, particularly through the engagement taken to *unidentify* a major part of the data processed. However, we pointed out that what is provided for, at best, amounts to partial anonymisation and thus data processed would still be personal data subject to the applicability of EU data protection legislation.

We recommended the several points in the text be clarified to better protect the data and fully anonymise them where possible. We also advised that the controller of every database is clearly identified, the period(s) for which the data is to be stored in databases is specified, the rights of data subjects and the security measures to be implemented are highlighted. Furthermore, we recommended additional safeguards for the transfer of data to third countries and to the processing of sensitive data.

3.9.2. Intelligent transport

On 13 June 2013, we published formal comments on two draft Commission regulations in the field of intelligent transport systems that were under scrutiny by the European Parliament and the Council. The draft instruments concern the collection and provision of information for road safety information services, one for general traffic information, the other on the parking options for trucks.

We were pleased to have been consulted during the drafting process and that data protection elements were taken into account in the Commission drafts. Road traffic information systems in the future are likely to rely more heavily on information collected via the multitude of mobile devices that will be installed in cars or carried by their drivers, such as location aware mobile phones, connected GPS navigation systems and other intelligent transport systems, such as cameras with number plate recognition capability.

We stressed the importance of data protection when much of the collected traffic data is related to identified or identifiable persons. We appreciate that these considerations are taken into account in the regulations, but explained that safeguards such as anonymisation of data become more difficult as more precise data is collected (*a study* on location data found that individuals can be identified from a very limited number of data points about their location, without any other information). The combination of data in traffic information systems, including the re-use of public sector information (Open Data) must, therefore, always be implemented with the appropriate data protection safeguards.

3.9.3. eCall

On 29 October 2013, we issued an Opinion on the Commission proposal for a Regulation concerning type-approval requirements for the deployment of the eCall system and amending Directive 2007/46/ EC. We stressed the potential intrusiveness of the 112 eCall system and even though we noted that many essential data protection safeguards had been specified in the proposal, we nevertheless insisted on complementary safeguards that should be included as well.

In addition, the mandatory fitting of eCall devices in all new vehicles by 1 October 2015 will not only allow the wider deployment and functioning of 112 eCall but will also provide an embedded geolocation platform to be used for private eCall services and added value services. We emphasised that any processing of personal data through the eCall in-vehicle system should comply with Directive 95/46/ EC. We therefore regretted that the data protection implications of these are not addressed in the proposal and called for the application of equivalent data protection safeguards to those services and specified these requests in our Opinion.

3.10. Other issues

3.10.1. Automatic exchanges of tax information

On 5 November 2013, we adopted comments on the Commission proposal for amendments to a Directive on the mandatory automatic exchange of information in the field of taxation. In our letter, we urged the legislator to specify the types of personal data that may be exchanged pursuant to the Directive and to better define the purposes and the context for which such data can be exchanged. We also emphasised that the principles of necessity and proportionality are respected under the Directive.

Moreover, we noted that neither the current Directive nor the new proposal contain provisions which spell out how the principle of transparency should be complied with in practice, for instance on whether (and how) the exchange of information is communicated to the public at large or how data subjects will be informed about the data processing. We therefore urged the legislator to adopt a provision in which the transparency of the proposed information exchanges is addressed.

3.11. EDPS access to documents policy

As an EU institution and according to our Rules of Procedure, the EDPS is subject to the Public Access to Documents Regulation (EC) 1049/2001. The number of public access requests for documents held by the EDPS is increasing progressively year by year. More precisely, this number has recently doubled from 14 requests in 2012 to 28 in 2013.

In 2013, we dealt with 4 confirmatory applications or requests for an internal review of the initial decision of an institution not to disclose or to only partly disclose a document. It is worth mentioning that 11 of these 28 requests were received via the Access Info website www.asktheeu.org. AsktheEU.org is a single portal for filing requests with EU public bodies. The goal is to make it easier for members of the public to ask for information.

We deal with requests according to our case manual on access to documents, which we adopted in 2012. This manual gives guidance to EDPS staff on how to deal with public access requests and is revised and updated periodically. In line with the manual, we also have a dedicated section on our website on the transparency policy of the EDPS.

The increasing number of access to documents requests we receive, underline the need for more detailed guidelines on the practical implementation of the Public Access Regulation, particularly those that concern the disclosure of personal data. Separate working level informal meetings have taken place between EDPS and the European Commission, the European Parliament and the Council of the EU. At the DPO meeting of 21 November 2013, these institutions requested that we take the lead in the organisation of a workshop, which will include the European Ombudsman (who have a special responsibility for transparency within the EU administration), to discuss the matter and develop guidelines.

3.12. Court matters

No EDPS decisions were challenged before the Court of Justice of the EU in 2013 and the EDPS did not instigate any proceedings against other EU institutions and bodies.

- **Digital Rights Ireland and Seitlinger and Others**

On 9 July 2013, the EDPS was invited to appear at a hearing before the Grand Chamber of the Court of Justice in a preliminary reference procedure. This hearing concerned Joined Cases C-293/12, Digital Rights Ireland, and C-594/12, Seitlinger and Others. Both cases relate to the validity of the Data Retention Directive 2006/24/EC.

It is the first time that the Court has invited the EDPS to attend a hearing in a preliminary reference procedure, to answer specific questions, on the basis of Article 24 of its Statute. In our submission, we emphasised the need to distinguish between Article 7 (*Respect for private and family life*) and Article 8 (*Protection of personal data*) of the EU Charter of Fundamental Rights. These provisions are closely related, but are quite different in nature. When determining the validity of legal acts under the Charter, the Court should therefore apply a double test, assessing whether the distinct requirements of both Articles 7 and 8 are fulfilled.

On 12 December 2013, Advocate General Pedro Cruz Villalón presented his Opinion in these cases. He noted that the Data Retention Directive pursues a legitimate objective, of ensuring the availability of traffic and location data for the purpose of the investigation, detection and prosecution of serious crimes. However, he advised that the Data Retention Directive constitutes a serious and unjustified interference with the fundamental right of citizens to privacy enshrined in Article 7 of the EU Charter of Fundamental Rights. In particular, he noted that when an act imposes obligations which constitute such an interference, the EU legislature should have provided for the necessary guarantees rather than leaving this responsibility to the member states. Among other things, the concept of serious crimes should have been more precisely described and at the very least, basic principles governing access to and the use of the retained data should have been set out in the Directive itself.

For the EDPS, this is an important step that may lead to a landmark decision on an issue that we have been following closely for a number of years. We are curious to see if the Court follows the Advocate General's reasoning.

- **Commission v. Hungary**

On 15 October 2013, the EDPS appeared at the hearing of *Commission v. Hungary* (Case C-288/12). This case is the third infringement case concerning the independence of data protection authorities, the other two being Commission v. Austria (C-614/10) and Commission v. Germany (C-518/07) for which rulings were given in 2012 and 2009 respectively. In our pleadings, we argued that Hungary had failed to fulfil its obligation to ensure that the national supervisory authority acts with complete independence. A change in legislation cannot in itself justify the termination of the mandate of the supervisory authority. The fact that the changes were made at constitutional level should not stand in the way of the primacy of EU law. The ruling is expected early 2014.

The other cases in which the EDPS intervened are still pending.

- **Pachtitis v Commission and EPSO (T-374/07) and Pachtitis v Commission (F-35/08)**

The applicant, Pachtitis, asked for an annulment of the decision by EPSO to refuse his request for the exam questions from the general competition (EPSO/AD/77/06) in which he had participated. The EDPS intervened in support of the applicant, pleading that the questions are an integral part of his personal data and thus refusing access implies a violation of the obligation to apply Regulation 45/2001 ex *proprio motu*.

On December 2011, the General Court contacted the parties to ask whether 'the legitimate interest' of the applicant should be revised in this case in light of the judgment in case T-361/10P[7]. Our position on the matter is that Mr. Pachtitis' request to access the questions remains legitimate.

- **ZZ v. EIB (Case F-103/11)**

During an internal harassment investigation conducted by the EIB, the full complaint on the alleged harassment, including the documents attached to it (which included medical declarations) was sent to the alleged harassers. The applicant claimed before the Civil Service Tribunal that this was contrary to Regulation (EC) 45/2001.

In June 2012 the EDPS submitted a written intervention supporting the applicant, as the claim was based on an alleged breach of these data protection rules.

7 In its judgment of 14 December 2011 in the case T-361/10P the GC states that "the legitimate interest of the applicant should be examined both in view of the day the application is filed as well as the day the hearing takes place". The Court stated that "the legitimate interest may be eliminated in the process due to objective or subjective reasons".

Dennekamp v. European Parliament

The EDPS recently submitted written arguments in the '*Dennekamp II*' case, (Case T-115/13, *Dennekamp v. European Parliament*), which concerns the need to find an appropriate balance between public access and data protection. The applicant, a Dutch journalist, requested a series of documents containing information on the membership of MEPs to the Voluntary Pension Scheme (including a list of names) from the European Parliament. In Dennekamp I, the Court ruled in favour of the Parliament, considering that the defendant had not provided explicit, legitimate justification to demonstrate the necessity for the information to be transferred to him.

In our written submissions in Dennekamp II, we address the necessity of the transfer for reasons closely related to the general interest of transparency. The EDPS considers that accepting this necessity would not amount to a special access right for journalists but would merely reflect the unique role of journalists as public watchdogs; in recognising the importance of the right of freedom of expression in a democratic society we support that, in situations such as this, the balance between the different interests at stake should be in favour of openness.

In October 2013, the EDPS asked for leave to intervene in two cases:

- **Elmaghraby and El Gazaerly v. Council of the European Union (Case T-319/13)**

The applicants in this case requested the General Court to annul a Council Decision concerning restrictive measures against certain persons, entities and bodies in view of the situation in Egypt and erase the allegations that each applicant is responsible for the misappropriation of State funds and is subject to judicial investigation in Egypt. The applicants pleaded violation of data protection rules according to the data protection Directive 95/46 and Regulation (EC) 45/2001.

The EDPS considers that this case offers an opportunity to assess the data protection challenges raised by the restrictive measures adopted by the EU institutions.

- **CN v Parliament (Case T-343/13)**

The applicant seeks compensation for the material and non-material damage suffered as a result of the publication of an extract from a petition submitted by the applicant containing items of personal data (including his state of health and the fact that there is a disabled individual in his family) on the European Parliament's website. The EDPS has requested leave to intervene in favour of the order sought by the applicant.

3.13. Priorities in 2014

In December 2013, the EDPS published his seventh public Inventory as an advisor on proposals for EU legislation, setting his priorities in the field of consultation for the year ahead. The EDPS faces the challenge of fulfilling his ever-increasing role in the legislative procedure while guaranteeing high-quality and well-appreciated contributions to it, to be delivered with limited resources.

The following main trends have been identified as predominant for 2014.

1. The debate following the revelations of mass surveillance has shed more light on practices on both sides of the Atlantic. In this context, strengthening privacy and data protection as fundamental rights has become an even higher priority on the EU political agenda. Data protection has been mentioned as a key issue in the talks preparing the establishment of a EU-US Free Trade Area and the Safe Harbour agreement between the EU and the US is currently under review. In particular, the debate triggered by the revelations concerning the programmes run by both foreign and EU intelligence services has contributed to raising privacy and data protection awareness in the public eye, a trend which encourages the EDPS to provide further guidance and input to the EU legislator and other stakeholders. As a first step, we will react on the Commission communication of 27 November 2013 on rebuilding trust in EU-US data flows, also taking into account the outcomes of the LIBE Committee inquiry into the electronic mass surveillance of EU citizens.
2. There is an increasing tendency of endowing administrative authorities (both EU and national) with effective information gathering and investigative tools. This is particularly the case in the area of freedom, security and justice and in relation to the revision of the legislative framework concerning financial supervision. In this context the increasing importance of 'internet monitoring', by public authorities as well as by private parties, is to be carefully considered in relation to irregularities on the internet.
3. An enormous amount of personal information is shared every day on the internet. Volumes of per-

sonal data are collected by companies to preserve and enhance existing client relations and for acquisition of new relationships. This personal data can be sold to other interested parties and has in effect become an intangible asset not accounted for on company balance sheets. Further use of these masses of information for law enforcement purposes may also take place. In view of these developments, issues such as the relationship between data protection and competition law are increasingly important. Following our Opinion on cloud computing, we plan to publish an Opinion on the role of data protection in EU competition law and we plan to do further work in the areas of Big Data and data as a currency.

4. EU legislation increasingly facilitates significant exchanges of information between national authorities, quite often involving EU-bodies and large-scale IT databases (with or without a central unit) of increasing size and processing power. This trend is likely to continue in 2014 in the context of the new programme for the Area of Freedom, Security and Justice (post-Stockholm). It therefore requires careful consideration by policy makers and actors in the legislative procedure when setting out data protection requirements, because of the important consequences these exchanges can have for the privacy of citizens, for example, by facilitating the monitoring of citizens' lives.

5. In order to ease the fiscal burden imposed on EU citizens by the financial crisis, member states are increasingly coordinating their action against tax fraud and tax evasion at EU level, by boosting the effectiveness of the tools of administrative cooperation in the tax sector - as was the case at the G20 with initiatives against bank secrecy. At the same time, the EU has started negotiations with some third countries for the conclusion of international agreements aiming to combat VAT fraud through the exchange of tax information. Although justifiable on grounds of compelling public interest, these initiatives need to be aligned with the rules on data protection, particularly with the principle of proportionality. These will be high on the EDPS agenda in 2014.

The EDPS is committed to devoting substantial resources in 2014 to the analysis of proposals of strategic importance. Additionally, the EDPS has identified a number of less obvious initiatives of less strategic importance which may become relevant for data protection. The fact that the latter are included in the EDPS Inventory implies that they will be regularly monitored, but does not mean that we will necessarily issue an Opinion or formal comments.

The main EDPS priorities, as identified in our inventory, are:

a. Towards a new legal framework for data protection
   - Proposals for a general data protection regulation and for a directive in the area of criminal justice from 25 January 2012.
   - Upcoming proposals, in particular relating to data protection in EU institutions and bodies

b. Rebuilding trust in global data flow in the aftermath of PRISM
   - Follow up of the Commission communication of 27 November 2013 on rebuilding trust in EU-US data flows
   - Review on the implementation of the PNR Agreement;
   - Analysis of the functioning of Safe Harbour

c. Initiatives to bolster the economic growth and the Digital Agenda
   - Single market in telecommunications (e.g. IP rights, network and information security, data protection)
   - Proposals on eProcurement, eHealth, Open Data
   - Review of competition rules
   - Cyber-security
   - Cloud computing

d. Further developing the Area of Freedom, Security and Justice
   - Post Stockholm Programme
   - Reform of agencies and bodies (e.g. Eurojust, OLAF, EPPO)
   - Initiatives against terrorism and extremism
   - Negotiations on agreements with third countries on data protection

e. Reform of the financial sector
   - Regulation and supervision of financial markets and actors
   - Banking supervision

f. Tax fraud and banking secrecy
   - Towards a definitive VAT system
   - Negotiations on agreements with third countries on the exchange of VAT information
   - Banking secrecy

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.

Our guiding principles

- we build on our expertise and experience in European data protection law and practice;
- we seek to improve consistency in data protection law across the EU.

4.1. Article 29 Working Party

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.

In 2013, we continued to actively contribute to the work of the Article 29 Working Party, in particular, through participation in thematic subgroups such as: borders, travel and law enforcement, eGovernment, financial matters, future of privacy, international transfers, key provisions and technology.

In particular, we acted as a rapporteur or co-rapporteur for the Opinions on purpose limitation[8] and on legitimate interest in the key provisions subgroup. This subgroup has been entrusted by the plenary with the drafting of substantial Opinions interpreting the essential principles of the data protection Directive, with the aim of providing consistent interpretation of current rules and recommendations for the future reform of the EU data protection framework.

We have also been closely involved in drafting two Opinions on the smart grid data protection impact assessment template[9] (technology subgroup) and the Opinion on open data[10] (eGovernment subgroup).

In addition to contributing to the on-going discussions on profiling, we devoted substantial resources to the following Opinions and working documents in 2013:

- Data protection reform discussions (implementing acts)[11];

8 Opinion 03/2013 on purpose limitation - WP 203.

9 Opinion 04/2013 and Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force - WP 205 and WP 209.

10 Opinion 06/2013 on open data and public sector information ('PSI') reuse - WP 207.

11 Working Document 01/2013 - Input on the proposed implementing acts - WP 200.

- guidance on cookie consent[12];
- apps on smart devices[13];
- mobile applications.

We also made significant contributions to several letters and analyses relating to the Snowden revelations and global surveillance, PNR agreements, API data, IATA new distribution capacity, transborder access to data in the framework of cybercrime, binding corporate rules (BCRs) and anti-money laundering issues.

We also cooperate with the national data protection authorities to the extent necessary for the performance of our duties, in particular by exchanging useful information and requesting or delivering assistance in the performance of their tasks (Article 46(f)(i) of Regulation EC (No) 45/2001). This cooperation takes place on a case by case basis.

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 EURODAC, the Visa Information System (VIS), the Schengen Information System II (SIS II) or the Customs Information System (CIS), which require a coordinated approach to supervision.

In 2013, we provided the secretariat for the new SIS II Supervision Coordination Group (SCG) and we chaired the EURODAC, VIS and CIS SCGs.

Changes in 2013 were accompanied by challenges for coordinated supervision. The new EURODAC Regulation[14] contained significant amendments, such as possible access by law enforcement authorities to EURODAC data. In addition, SIS II became operational. To reduce the financial, travel and administrative burdens, we established back to back meetings of the SCGs and aimed to ensure consistent, horizontal supervision policies of the large-scale IT systems where possible.

The SCG model will expand in 2014 with a new supervision coordination group for the Internal Market Information (IMI) System.[15] We therefore consulted national data protection authorities and the Commission in 2013 to take stock of the status and developments in the IMI Regulation in order to organise the first meeting for the group in 2014.

The coordinated supervision model has become a standard for the EU legislator and the Commission has proposed it in a number of proposals such as on Europol, smart borders, Eurojust and the European Public Prosecutor's Office.

4.2.1. EURODAC

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.[16]

We organised two meetings in Brussels for the EURODAC SCG, one in April and one in November 2013[17]. The group, composed of representatives

12 Working Document 02/2013 providing guidance on obtaining consent for cookies - WP 208 (02.10.2013).

13 Opinion 02/2013 on apps on smart devices - WP 202.

14 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), (OJ L 180/1, 29.6.2013)

15 Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC, OJ , L 316/1.

16 Iceland, Norway, Switzerland and Liechtenstein.

17 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/13-10-16_Eurodac_SCG_Summary_EN.pdf

from national data protection authorities and the EDPS, based its activities on its 2013-2014 work programme.

The EURODAC SCG working programme for 2013-2014 concentrates on the need to supervise the transition to the EURODAC rules that will come into effect in June 2015 according to the new EURODAC provisions.[18] The group also shared information about national inspections in different member states and was updated on recent developments by the Commission.

Unreadable Fingerprints Report[19]

Based on the analysis of the replies received, the report included several recommendations to competent authorities in the member states to establish clear and binding procedures.

These recommendations should allow asylum seekers to benefit from harmonised practices throughout the EU (avoiding possible discrimination). The procedures should clarify that unreadable fingerprints are not to be used per se against applicants, but that any adverse consequences for applicants need to be justified by sufficient evidence.

One of the recommendations for best practice is to oblige competent authorities in the member states to retake fingerprints after a given time (for example two weeks) in order to allow the ridges to regenerate and, if possible, involve a specialist forensic or technical officer at the procedure. To decrease the administrative burden and related stress, a common minimum time for retaking fingerprints should be established. This will benefit asylum seekers as well as the national authorities. It should also be decided whether the applicant, when detained, is to be informed of the fingerprint retaking.

Asylum seekers should also be assured of the right to lodge a complaint against the relevant national authorities or even national data protection supervisory authorities.

The next meeting of the EURODAC SCG will be held in spring 2014.

18 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0001:0030:EN:PDF

19 https://secure.edps.europa.eu/EDPSWEB/edps/cache/off/Supervision/Eurodac

4.2.2. VIS

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 eight other regions.[20]

The VIS SCG is composed of representatives of the national data protection authorities and the EDPS. We organised two meetings in Brussels for the VIS SCG, one in April and one in November 2013[21], both as back-to-back meetings with EURODAC and SIS II SCG meetings.

The VIS SCG adopted its Rules of Procedure and the Working Programme for 2013-2014. The focus of the working programme is to strengthen the cooperation in inspections by establishing a common format for national inspections, to study the cooperation between member states and external providers and how data protection is applied in the processing of visa applications.

Several members of the group were tasked to start work on a study on the cooperation between member states and external providers and to discuss the long term perspective of supervising the VIS.

VIS SCG members also shared information about national inspections in the different member states. The group was updated on the status of the VIS roll out and other recent developments that impact data protection by the Commission.

The next meeting of the VIS SCG will be held in spring 2014, as a back-to-back meeting with the other large-scale IT systems SCGs (EURODAC and SIS II).

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

21 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/VIS/13-10-16_VIS_SCG_Summary_EN.pdf

4.2.3. CIS

The aim of the Customs Information System (CIS) is to create an alert system within the framework of combating fraud so that any member state can request another to carry out sighting and reporting, discreet surveillance, a specific check or operational and strategic analysis through the system.

The CIS stores information on commodities, means of transport, persons and companies and on goods and cash detained, seized or confiscated in order to assist in preventing, investigating and prosecuting actions which are in breach of customs and agricultural legislation (the former EU first pillar) or serious contraventions of national laws (the former EU third pillar). The latter is supervised by a joint supervisory authority (JSA) composed of representatives of the national data protection authorities.

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[32]. The EDPS and national data protection authorities cooperate in line with their responsibilities in order to ensure coordinated supervision of CIS.

The Coordination Group shall:

- examine implementation problems related to CIS operations;
- examine difficulties experienced during checks by the supervisory authorities;
- examine difficulties of interpretation or application of the CIS Regulation;
- draw up recommendations for common solutions to existing problems;
- endeavour to enhance cooperation between the supervisory authorities.

In 2013, we organised two meetings in Brussels for the CIS SCG Group.

The sixth meeting of the CIS SCG took place in June 2013. As the mandates of the Chair and Vice Chair had expired, an election was held by means of a secret ballot. Mr. Giovanni Buttarelli, Chair of the Group, and Mr. Gregor König, Vice-Chair of the group, were both re- elected.

The group also studied the draft report on the coordinated inspection of the list of authorities having access to CIS and FIDE and the draft report on CIS data subjects' rights.

In the December 2013 meeting, due to the departure of Vice-Chair Gregor Konig, a new Vice-Chair was elected. We updated the group on the inspection of the CIS. The Commission presented recent developments regarding Council Regulation 515/97, on the technical developments of the CIS and, in particular, on the state of play of the publication of the list of authorities having access to SIS/FIDE. The group reflected on possible issues to be put on the work programme for 2014-2015.

4.2.4. Schengen Information system

The Schengen information system (SIS) is a large scale IT system created following the abolition of controls at internal borders within the Schengen

22 Regulation (EC) No 766/2008 of the European Parliament and of the Council of 9 July 2008 amending Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters.

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 second generation system SIS II became operational in May 2013, thus replacing the aforementioned SIS, and consists of a central database called the Central Schengen Information System (C-SIS) for which the Commission ensures operational management connected to national access points defined by each member state (NI-SIS).

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.

The Coordination Group shall:

- examine implementation problems related to SIS operations;
- examine difficulties experienced during checks by the supervisory authorities;
- examine difficulties of interpretation or application of the SIS Regulation;
- draw up recommendations for common solutions to existing problems;
- endeavour to enhance cooperation between the supervisory authorities.

In April 2013, the SIS II SCG took over the SIS joint supervisory authority and held its first meeting in June and its second in October, both in Brussels. In the June meeting, the agenda dealt with administrative matters: the election of a Chair and Vice-Chair, in which Ms. Clara Guerra representing Portugal's DPA and Mr. David Cauchi representing Malta's DPA were elected respectively; the adoption of the rules of procedure for the group and the recognition of the observer status of Bulgaria, Cyprus, Ireland, Romania and the UK.

More substantive issues such as the hacking of the Danish NI-SIS, the state of play of the SIS II migration process and a SIS II information campaign were also discussed. Future steps to be taken by the Commission and eu-LISA regarding the SIS II security policy in particular and future activities of the supervision coordination group for 2013-2014 were also addressed.

In the October meeting, the group again discussed the hacking of the Danish NI-SIS and the necessary involvement of the SIS II SCG in the follow-up to the incident. This was emphasised to the Commission who attended the meeting to present the outcome of the work of the SIS II security subgroup it had set up following the hacking.

The SIS II draft working programme was also discussed by the group together with a possible framework for audits common to SIS II, VIS and EURODAC SCG and the establishment of an expert subgroup common to SIS II, VIS and EURODAC SCG.

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.

In 2013, the European Conference of Data Protection Commissioners took place in Lisbon on 16 and 17 May. The conference concentrated on several themes connected to the recent developments for the modernisation of the data protection frameworks of the EU, the Council of Europe and the OECD. In particular, the concepts of personal data, the rights of individuals on the internet and information security were discussed.

The conference also addressed how to strengthen the supervision and cooperation of data protection authorities, the consistency in the role and competences of data protection authorities and how they could better cooperate and ensure leadership.

The conference adopted three resolutions, one on the future of data protection in Europe, another on data protection in a transatlantic free trade area and the third on an adequate level of protection at Europol.

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.

35th INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS
PRIVACY: A COMPASS IN TURBULENT WORLD
Warsaw, 23-26 September 2013

The 35th Annual Conference of Data Protection and Privacy Commissioners took place in Warsaw on 22-26 September 2013. The conference concentrated mainly on the reforms of data protection across the world (particularly those in the EU, the Council of Europe and the OECD), the interaction with technology and the roles and perspectives for different actors, including data subjects, data controllers and supervisory authorities. The list of distinguished speakers included Peter Hustinx, EDPS and Giovanni Buttarelli, Assistant EDPS.

At the conference, a series of resolutions were adopted, including on the 'appification' of society, on profiling and on international enforcement coordination.

International enforcement coordination was discussed at the last conference in Uruguay and its importance has been confirmed by the on-going work of the Enforcement Coordination Working Group (IEWG), tasked with investigating common ground for cooperation between supervisory authorities worldwide. We participate in the International Enforcement Cooperation Working Group and contribute to the analysis of options for and barriers to enforcement cooperation. The next international enforcement conference will be held on 3 and 4 April 2014 in Manchester.

Additionally, a resolution was adopted on *anchoring data protection and the protection of privacy in international law*. This resolution came as a reaction to the revelations of global surveillance by US intelligence services over the course of the summer, with a view to ensuring recognition at international level of these fundamental values.

Many side events were organised before or in parallel to the conference, such as the Public Voice Conference with the participation of civil society actors and the Phaedra conference dedicated to the development of international enforcement cooperation.

The 36th International Conference will take place in Mauritius in October 2014.

4.5. Other international cooperation

4.5.1. Council of Europe

The Council of Europe Convention on Data Protection (Convention 108) of 1981 is the oldest binding international instrument on the subject and has also inspired Directive 95/46/EC. It aims to strengthen data protection for individuals in light of the increasing flow of data across borders in automated processes. In our capacity as an observer with the right to intervene, we attended two meetings of the Consultative Committee of Convention 108 in May and October 2013. It was particularly important for us to attend these meetings to be able to follow and play a part in the on-going modernisation of the Convention.

Since the adoption of the amending protocol to the Convention at the meeting of the Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (T-PD) of November 2012, our comments have focused on the explanatory report. We also participated as an observer at the meetings of the ad hoc committee on data protection (CAHDATA) which pursues the work of the T-PD at ministerial level. We provided comments to strengthen data protection by harmonising the proposed text to ensure consistency both within the Convention and with the future data protection framework at EU level.

In addition to following the work of the T-PD and the CAHDATA, we participated in the discussions of the Committee of the Convention on Cybercrime. As rapporteur, we contributed to written

comments on the possible revision of the Convention on cybercrime sent by the Article 29 Working Party to the bureau of the Committee. We also follow the work of the Steering Committee on Media and Information Society (CDMSI).

4.5.2. OECD

We formed part of the experts group tasked with updating the privacy guidelines (Privacy volunteer group - WPISP) of the Organisation for Economic Co-operation and Development (OECD). This group of experts, chaired by the Privacy Commissioner of Canada, Jennifer Stoddart, was composed of representatives from governments, privacy enforcement authorities, academia, industry, civil society and the internet technical community.

As a member of this group, we attended several meetings and contributed written comments to the draft update of the guidelines. Among the issues addressed were the strengthening of the role of supervisory authorities, the accountability of data controllers and the enhancement of legal certainty with regard to data transfers. The revised guidelines were adopted on 11 July 2013 [23].

4.5.3. APEC

The 21 countries of the Asia-Pacific Economic Cooperation (APEC), which include the United States, Canada, Japan, China, Russia, South Korea and Australia, have developed a system for cross-border privacy rules (CBPR) to protect privacy and guarantee data transfers.

The CBPR are similar in some respects to the binding corporate rules (BCR) that are used for European data transfers. For example, both apply to international transfers developed by companies and are first reviewed by data protection authorities or by authorised third parties.

The Article 29 Working Party has been closely following the development of CBPRs and together with APEC countries, jointly analysed the possible adoption of a common referential for industry, highlighting the similarities and divergences between the two systems. In this context in 2013, we provided substantial input to the discussions and drafting work of the APEC Privacy subgroup and in the EU-APEC meetings towards a dual 'certification' for CBPR-BCR compliance procedures.

4.5.4. Association Francophone (AFAPDP)

The main aims of the French-speaking Association of Personal Data Protection Authorities are to launch a debate about the challenges facing data protection in French-speaking areas, as well as the creation of a network for exchange and cooperation amongst the independent data protection authorities.

One of our particular contributions to their annual meetings has been to explain the EU framework to countries which are developing data protection legislation, such as Morocco and Burkina-Faso. Last year's meeting took place in Marrakech on 20 and 21 November 2013.

4.5.5. 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, the Americas and Asia as well as privacy experts from industry.

We take part in their meetings and contribute to the documents prepared by the group which in 2013, included working papers on web tracking, indexing and aerial surveillance drones. A working paper on the right to telecommunications privacy served as the basis for a resolution proposed at the international conference.

23 OECD guidelines governing the protection of privacy and transborder flows of personal data, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

5 MONITORING TECHNOLOGY

Our strategic objective

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

5.1. Technological development and data protection

In 2012, we adjusted our internal organisation structure and established an IT Policy team to provide relevant expertise and insight and reinforce our capacity to monitor technological developments. 2013 was the first full year of activity for the team to assess the impact of developments in technology on data protection and privacy. This on-going monitoring has contributed to building and maintaining the necessary expertise for us to adequately perform supervision, consultation and cooperation tasks that require technical analysis.

The IT Policy team also scrutinises the choices to be made for our own IT needs, so as to ensure that we not only follow our own recommendations, but also apply best data protection practice.

One of the key issues in the development of internet technology is that developers of new standards, tools and services presently receive little advice from data protection experts on practical ways to implement privacy friendly solutions. A wider discussion on the technical approach to privacy could help to explain the principles to developers and explore the options for systematically integrating data protection at the development stage and help programmers understand how they can apply the principle of privacy by design in their practical work.

Strengthening our contacts with technology experts in the EU bodies under our supervision, as well as in the private sector, academia and others, could therefore help to improve technical support for data protection and highlight the technical options to privacy experts. As an example, the preparatory work on our Guidelines for websites and mobile device usage has

- 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 seek to improve our technical supervision capabilities and provide guidance on technical aspects of data protection compliance to data controllers. We also offer technical advice as part of specific Guidelines.
- 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 apply data protection principles to our own internal IT issues, such as the hosting of the case management system.

already led to more focused discussions on specific technical and data protection issues.

Contributing to these discussions and promoting privacy friendly technology, in cooperation with other data protection authorities, will remain an important area of activity.

This chapter presents observations from our technology monitoring and highlights selected developments with particular relevance for privacy and data protection.

5.2. Internet security and surveillance

Securing the internet has been an on-going endeavour since its inception; the ever changing nature of the internet (size and use) and the changes in the nature of threats ensure that security will continue to preoccupy different communities. Recent reports about the pervasive monitoring of internet traffic have, however, surprised many since its scale was not anticipated in the design of many internet protocols. These revelations have illustrated that many operational practices today leave end users vulnerable and unsettled in their trust of the digital market place. While some of the attacks are fairly sophisticated, the majority have exploited rather basic security vulnerabilities that are also regularly exposed when data breaches occur.

In this section, we will focus on the technical aspects, particularly in those areas where internet security has been challenged. Improvements in these areas will improve protection against a wide range of attacks and make unauthorised access more difficult and increase the cost for attackers. At the meeting of the Internet Engineering Task Force (IETF) in Vancouver in November 2013[24], the engineers designing internet protocols agreed that massive access to metadata (traffic and location data) on the time and place of communications and to the actual content of communications should be considered an attack and their threat model needs to be adjusted accordingly.

5.2.1. Cryptographic Primitives

Cryptographic primitives are well-established, low-level cryptographic (coded) algorithms that are frequently used to build computer security systems. Internet security relies on sound cryptographic primitives, such as hash functions, random number generators, integrity and encryption algorithms, etc. These primitives provide the foundation for secure communication over the internet and serve as building blocks for more complex systems. Cryptanalysis aims to break these security systems and there have been various advances by researchers (with ciphers such as RC4) but the full capabilities and knowledge in this area remain unknown. In addition to potential advances in cryptanalysis, rumours about backdoors in specific elliptic curves and random number generators have created some uncertainty about which algorithms are 'safe' to use and what influence there has been on the standardisation process.

5.2.2. Protocols and Architecture

Communication on the internet relies to a great extent on standardised protocols - a system of digital rules for message exchange within or between computers - such as HTTP used for the web platform, TLS as a common tool for securing web transactions and all the email protocols. Cryptographic primitives are building blocks in those communication protocols. Underlying these protocols is an architecture that allows communication on the scale of the internet.

24 http://www.ietf.org/mail-archive/web/ietf/current/msg83857.html

An architecture combines a number of individual building blocks to create something larger. The web 2.0 architecture, for example, not only utilises HTTP but also builds on HTML, on the use of JavaScript and on TLS for security.

Industry trends have led to a more server-centric design where data is frequently stored in a central cloud service (instead of following a peer-to-peer paradigm). Interconnecting different applications on the web has become the norm in so-called mash-ups. This has, however, simplified interception and surveillance since data can be collected on a large scale from a small number of companies.

In the design of some communication architectures, such as VoIP or even email, little attention has been paid to avoid the easy collection of traffic data. Traffic data, often referred to in public discussion as metadata in comparison to the actual communication content, provides information about when, where and with whom an interaction takes places. It turns out that this traffic data in itself is of great value for analysts.

In many cases end users are left with a limited choice of either uploading their data to an application or not using the application at all. It is likely that this trend will continue, since businesses also see great value in big data analysis which requires a massive collection of data about their users. These massive data collections are of course very valuable targets for attackers.

5.2.3. Implementation

Once the protocols and the architectures have been developed (typically by standards organisations), the specification needs to be turned into code. Producing high quality code is difficult and requires skilled programmers and processes that ensure sufficient testing and quick reactions to bug reports.

Unfortunately, implementation may reveal a number of security weaknesses, such as lack of security features, including security vulnerabilities (as illustrated in the top 10 security vulnerabilities of web applications), weak pseudo-random number generators and even trojans in hardware before it is shipped to customers. Backdoors can also be added to software, particularly since many product implementations are not publicly available.

These security vulnerabilities can be exploited by a number of actors, including criminals.

5.2.4. Deployment

Once a product or service has been implemented it can be deployed, for example via a smart phone application or web service. Many important design decisions that have to be made during this phase can impact privacy and security. For example, an email provider can decide on the location of its server infrastructure, whether confidentiality protection will be made available to each communication and how strong authentication will be. For other products, decisions have to be made about the hardware and software platform.

The security practices of companies and the weak security of products have made it easy to compromise networks and user data. This has severely affected confidence in internet communications.

In response, researchers and internet protocol architects are reflecting on how to design a system that benefits society but also protects individuals.

The list of possible actions includes:

- using transparency and openness in standards processes to ensure that a single party is not able to hijack the process and negatively impact the standardisation results;
- increasing the use of open source software, which allows those who are interested to inspect the source code of products and makes it more difficult to install backdoors and often increases the quality of the code;
- increasing security and privacy in the design of internet protocols. This includes the design of better end-to-end security techniques and alternative communication architectures that produce less metadata at intermediaries;
- promoting state initiatives to improve the deployment of services that respect security and privacy;
- increasing the diversity of service offerings. As an example, a larger number of email and social network providers mean that more targets need to be attacked to access the data of an equivalent number of internet users.

At the same time, companies need to change their practices and address internet security and privacy more seriously. Otherwise consumers will hesitate to download a smart phone app or sign up for the latest web service.

5.2.5. Anonymisation

With the data protection reform underway, some topics such as the right to be forgotten and profiling have been the subject of intense debate. Anonymisation of data will have a profound impact as a result of the new legislation, as it is a core data protection concept: what is personal data and what is truly anonymous data[25].

Some in the debate believe that there are different types of data that should be protected according to the estimated risk to that data, the so-called *risk-based approach*. With this approach, anonymous data by definition cannot be traced back to an individual, or, in reality, has been made very difficult to re-identify an individual, and thus, can be processed freely and do not require a high level of protection. On the contrary, data that relate to an identifiable individual must adhere to the data protection framework.

This has sparked a debate to make the processing of personal information more flexible by introducing the notion of pseudonymous data. In a pseudonymous data set, the identifying information would be replaced by a pseudonym. This would make identification of a specific individual more difficult. It is important to note, however, that because pseudonymised data can be linked to an individual, it is still personal data. One typical example is medical research where patients are not known directly to the researchers, but only through their medical attributes. A number is used to differentiate each patient's data and a limited set of people are authorised to know the correspondence between this number, the name and date of birth of the patient.

Attempts have been made to include a definition for pseudonymous data in the new data protection Regulation. However, Opinions are divided on the matter: some take the view that this approach weakens data protection[26]. On the other hand, some companies anticipate business opportunities with the introduction of pseudonymous data which will allow the extensive processing of data[27].

> *Until recently it was believed that de-identification could be a powerful tool to protect privacy. However the rise of* big data *is making de-identification increasingly difficult. As more and more data will be collected in future, it might very well become impossible to anonymise data*[28].

From a data protection perspective, the use of pseudonymous data could be useful as an additional control to protect personal information and minimise the risks, but it should be emphasised that pseudonymous data is still personal data and must be protected accordingly[29].

What is still needed is a detailed analysis of the techniques used to de-identify data and further work on how to implement these techniques. For example, one of the advanced techniques is *differential privacy*. Differential privacy allows a third party to query a database through an intermediate layer that will distort (to some extent) the results so as to protect the identity of the data subject. The more a third party queries the database, the more distorted the data becomes. This technique has been studied for a number of years and has a mathematical basis. However, the implementation of this technique is no small matter[30] and it might not be suitable for all types of personal data.

Furthermore, for some types of data, for example location data, de-identification might prove to be

25 http://www.theguardian.com/news/datablog/2013/aug/12/europe-data-protection-directive-eu

26 http://www.cepis.org/index.jsp?p=636&n=639&a=4696

27 http://euobserver.com/justice/119148

28 https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable

29 http://pdpecho.wordpress.com/2013/03/13/reding-on-pseudonymous-data-we-should-encourage-companies-to-use-pseudonyms-rather-than-the-actual-names/

http://www.huntonprivacyblog.com/2013/03/articles/european-data-protection-supervisor-issues-additional-comments-on-eu-data-protection-reform-package/

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_reform_package_en.pdf

30 http://www.cis.upenn.edu/~ahae/papers/fuzz-sec2011.pdf

incredibly difficult, as a recent MIT study illustrates[31]. In this study, the location data of individuals (for example collected from mobile phone connections to cell towers) was analysed. Surprisingly, 95 % of these data subjects can be identified with only 4 entries in a data set consisting of 15 months of mobility coordinates of 1.5 million people in space and time for an area comparable to a region of a member state.

Further discussion is needed in this field and guidelines for data controllers on how to anonymise different types of personal data, such as financial, health and telecommunication data, will be necessary[32].

While techniques will have to be developed and promoted to minimise re-identification risks, it is paramount that the protection provided by the legal framework remains intact. Many actors would like to process more data with fewer controls and seek to obtain legal permissions for innovative ways to process information transformed into data sets that can only indirectly identify individuals.

Legislators must not re-draw the boundaries within which personal data is defined, reducing the protection of individuals. Re-identification of such data sets would remain possible, and privacy risks would even increase, given the increasing propensity to collect large amounts of information on everybody.

5.2.6. Tracking

Each access to a web page can be traced by the web server.

Many web users are unaware that browsing a website involves an interaction between their device (PC, tablet, smart phone etc.) and the server providing the web content. Unlike a TV or radio broadcast, a printed book or newspaper, a billboard or poster in the street, a web page is only made available following an individual request from the user's browser. This request must identify the user's device because otherwise the server would have no indication of where to send the requested page. This direct interaction allows a form of tracking at its most basic level, i.e. keeping a record of each request for a particular web page at a specific time.

The internet eco-system has evolved considerably since the days when web pages were static and looked the same for everyone. Today, pages are usually tailored for each user and contain targeted content, often with the aim of increasing the economic value of the page view, by displaying attractive commercial offers or by displaying advertising that draws the user's attention.

This customisation of pages requires much more information about the user than is provided through a simple request for a web page and has triggered the development and use of more sophisticated tracking mechanisms. Furthermore, the content of pages is no longer provided by just one server, instead several actors are involved, for example, the main content on news sites is news while different advertising providers fill the other parts of the screen; all of them hope to maximise the attention they get during the user's limited browsing period.

One of the most common tools, cookies, were standardised in 1995 to allow the storage of information about user preferences and behaviour across user sessions. Concerns over the increase in tracking have developed in parallel and ideas about a Do Not Track (DNT) mechanism were first presented by consumer groups in 2007.

In law, the 2009 amendments to the EU ePrivacy Directive aimed to increase transparency and user control of cookies and other tracking mechanisms which store information on the user's device. So far, these intentions have not been fully achieved, as many websites today only provide users with a general information banner indicating the use of cookies, but offer little detail or choice, other than not to use the website at all.

The increase in online businesses has led to an associated increase in tracking. Stricter rules on cookies have triggered the development of new tracking mechanisms, in order to circumvent these rules.

One alternative to cookies is device fingerprinting , which involves the collection of as many characteristics of the user device as possible, including technical

31 http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

32 In 2013, the Article 29 WP started working on such guidance.

elements such as screen size, browser and operating system type and version, installed fonts and add-ons and user preference settings such as language, zoom factor, character encoding and so on.

The more characteristics that are collected the more likely it is that no two different user devices have the same profile. While some servers use only those characteristics that the user or rather the user's device must provide to receive a webpage adapted to its preferences and capabilities (passive fingerprinting), others instruct the browser to execute code, such as JavaScript, to reveal additional characteristics (active fingerprinting) for a more comprehensive profile.

One of the organisations developing standards for the internet, the Worldwide Web Consortium (W3C), has made an effort to provide users with a way to communicate their desire not to be tracked by standardising a DNT header inside the main web protocol HTTP. These standardisation efforts have made slow progress and have not met several publicised deadlines, but there is hope that the final technical specification may be available in 2014.

Despite some doubts about tracking quality, the use of device fingerprinting is increasing, as a recent study by KU Leuven indicates[33].

In the meantime, some browser manufacturers have nonetheless included support for DNT in their products: Microsoft announced that DNT is turned on by default in IE 10 and in IE 11. Apple has not allowed third party cookies for some time in their Safari browser and in February 2013, Mozilla announced plans to turn third party cookies off, although their plans have been postponed. Apple has even added support for the DNT header outside the browser realm into the iOS 6 operating systems used by their smart phones.

However, completely new ways of tracking have also been developed and engineers have displayed great creativity in generating increasingly sophisticated ways of tracking, such as tracking the cursor movement on a user's screen. Distributed identity management solutions allow tracking across several web services. With identity management, users log onto a website using their credentials (typically a username and password) and are thereby uniquely identified, regardless of the device they are using. Identity management is necessary for personalised services, such as webmail or social networking services.

33 http://www.kuleuven.be/english/news/several-top-websites-use-device-fingerprinting-to-secretly-track-users

More and more services now require user identification, such as in gaming or content streaming. As users are unlikely to remember many and varied passwords for all the sites they log onto, distributed identity management systems have emerged. These systems allow users to re-use their accounts, e.g. from a social networking service, on multiple websites without having to create a new account on each site.

While there are many services on the web that offer re-usable identity management, websites would have to configure their service for each identity provider. In order to minimise the effort needed, providers limit their support to the most popular identity providers, so that the most supported identities are from Facebook and Google.

Distributed identity management solutions offer more powerful tracking capabilities than cookies and device fingerprinting since they are able to track users across several devices.

Browsers are only one way to access the web. Smart phone and tablet users may choose from huge catalogues of downloadable applications called apps. When apps are executed on a user's device, they are able to access a wide range of personal information. Smart phone and mobile operating systems (OS) manufacturers, like Apple, Google, or Microsoft, have designed tracking mechanisms into the OS and the hardware, to set up an infrastructure that allows an in-depth analysis of the tracked interactions, using unique identifiers integrated in the hardware.

Furthermore, application developers may also incorporate third party analytics software into their apps. Such software tracks users throughout their use and provides the app developers with indications on how they can make their apps more user-friendly, but at the same time gives the analytics software provider access to user data across many apps and devices.

The next challenge for tracking developers is to go beyond the use of the web through browsers and apps and capture online and offline behaviour.

Tracking and advertising are still developing in many areas, for example, in home entertainment systems and dedicated gaming consoles which offer an increasing number of services to applications, including identity management capabilities as well as advertising APIs. The use of games, as a sort of living lab, to test users' reaction to stimuli is an opportunity to find brand new ways of tracking, by using built-in cameras, for example.

The built-in intelligence and tracking capabilities of other consumer devices have increased as well. The traditional TV set is being replaced by devices with built-in capabilities to connect to the internet and search for program offers on dedicated web servers. Cable modems now usually work as internet devices as well and exchange information with the servers of the cable network operator, routinely identifying at least the household, for controlling access to value added or premium services according to their subscriptions.

This also provides media service operators with details on the media use of their customers, which in turn allows for a precise and comprehensive analysis of interests, habits, preferences and influences, from political programmes to advertising clips. While there has not been much research on the privacy and data protection impact of these developments, initial studies have raised considerable concern: an investigation of the Dutch data protection authority into a Dutch connected TV network discovered noticeable breaches of data protection law.

The collection of location data and its use for different business purposes continues to increase. The growing concentration in the market for mobile devices and communications services will further strengthen the role of the very few global players that act as collectors of location and other communications related data.

Other areas where there is an increase in geo-location tracking include bluetooth and WiFi tracking and the tracking of mobile phones at short distance by their radio signals or when they are triggered into interaction. In addition, many other devices are now equipped with communication and tracking capabilities, including biometric sensors used in sports, satellite navigation systems, automated toll payment systems and electronic tickets for public transport (see section 5.2.7 on the Internet of Things).

The increasing integration of communication, location and processing equipment in motor vehicles, such as is intended by the comprehensive roll-out of an eCall system in all new passenger cars in Europe from 2015, will create an interest in using this platform for purposes other than emergency services. Ideas for car insurance fees based on distances driven, taking account of the precise area travelled and the driver's behaviour (e.g. frequent acceleration and braking) are just some of the creative ideas for the use of travel data. There are increasing demands to use number plate recognition data from existing road toll systems for law enforcement or from speed control systems that recognise number plates of cars entering and leaving a highway to calculate their average speed on that section.

Commercial tracking tools also serve state surveillance.

Recent media publications show that tracking information is not only used for commercial purposes, but also by governments in augmented surveillance programmes. For example, cookie tracking may be used as a means to hack into a specific user's device and place hidden software that enables remote exploitation. Google's tracking cookie, PREF, has been used to target communications activities on the computers of specific users and the location of mobile users has been tracked via mobile applications. The implications of commercial tracking on the fundamental rights to privacy and data protection are not limited to the interests of business.

5.2.7. The Internet of Things

The term *Internet of Things* (IoT) was chosen to denote a vision of a future in which everyday objects such as phones, cars, household appliances, clothes, transport and logistics are wirelessly connected to each other using internet technology, allowing them to share data and interact with each other. For example, IoT is used in innovative concepts such as *Smart Cities* where data is collected with the intention to alleviate urban problems, such as traffic jams and environmental pollution. This vision of IoT was the driving force for policy, research and development efforts to develop governance structures and common principles for a wide range for devices and services.

Many questions have been raised over the last ten years. How will the IoT change the internet as we know it? Will new protocols for IoT communications be needed? Will the existing governance model

apply to communications device manufacturers and service providers as well as to all manufacturers of consumer devices? How will consumers (and others) be involved? What standards are necessary?

As yet, there is no single IoT (or Machine-to-Machine, M2M) standard available. Instead, a wide range of different standards have been developed for different purposes.

Instead of waiting for the new comprehensive IoT architecture to emerge, many companies have been building operational IoT solutions on the basis of existing internet protocols and applications to connect them to existing internet infrastructure. While this pragmatic approach appears rather straightforward, it has long been believed that the masses of small sensors and actors that make up the IoT require specific new communication standards and mechanisms.

Some practitioners believe that the growing number of working solutions demonstrate that the existing internet protocol infrastructure can support the development of IoT solutions. Even though this approach may lead to a number of separate 'island' solutions initially, for certain industry sectors or fields of application for instance, it seems they could lead to economically viable business models which offer serious competition in the development of a holistic model for IoT.

As a result of this pragmatic approach, we have seen the emergence of a wide range of devices that collect information about individuals and upload it to various web services, for example, in wearable sports monitoring equipment. To facilitate these developments, companies have had to develop a systems design that would work within the limited capacities of small devices in the absence of a protocol and which supports direct communication between devices of different types from different manufacturers. Sensors rarely interact with each other 'peer-to-peer' but instead submit data via centralised services through cloud computing environments.

While this centralised design simplifies the management of security and access control, it has a profound impact on data protection and privacy, by creating huge collections of personal data that could be used for further analysis and exploitation. IoT devices behave like many other internet services, in that the maximum data available are collected rather than the minimum needed. Users are still accepting this trend, but the privacy concerns over cloud computing and big data analytics apply equally to the IoT.

Applying the established data protection principles of data minimisation and purpose limitation would be an effective safeguard against the most significant privacy risks. Unfortunately, these have not been guiding principles in the development of the internet, nor in the design of mobile device applications. The same indifferent approach is likely to be carried over to the IoT as well. At present, there is little or no incentive for the service provider who writes the software for IoT devices to take privacy and security issues seriously, especially since existing standards do not take account of these objectives.

Security also remains a challenge. Experts are concerned that we are building the next generation of critical, but insecure infrastructure due to the relaxed practices of embedded devices[34]. To lower the development cost of these small devices, savings are often made in the area of security. It remains to be seen whether current efforts to raise the awareness of this growing risk, will help to educate the global IoT development community on better security practices.

In the meantime, technological alternatives exist in the open source area. Affordable devices (approximately 20–40 EUR) allow consumers with a little IT knowledge to experiment with their own IoT ideas. Devices such as Arduino and Raspberry Pi are popular in schools and are used to introduce computer science concepts to children and teenagers. On the server side, an enormous collection of web and cloud software exists. Privacy aware developers working with these tools could develop privacy friendly solutions to serve as examples of best practice or as alternatives to industry products.

5.3. Biometrics

5.3.1. Personal genomics

In 2003, a scientific research team successfully completed the human genome project, the sequencing of all human genetic information. As a result, genetic testing is now widely available. The testing involves a small area of the entire genome, but the results, which are highly accurate, can often be delivered in a matter of days.

The sequence of DNA in our genes determines our ability to survive and reproduce. In humans, approximately 3 billion DNA base pairs make up the genome

34 http://www.wired.com/Opinion/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

and tiny variations give rise to a unique code for each of us. This vast volume of information in an individual's genome is the biometric equivalent of his or her identity. It may serve as a biometric identifier, since it is difficult to anonymise the information contained in a genome. It is clear that personal genomics represent a challenge for personal data protection.

Genetic testing is being used in medical research to identify the mutations in our genes to help develop therapies that will prevent diseases such as cancer, Alzheimer's, heart disease and others. There are many other possible uses for genetic information, some with significant implications for privacy. For example, there is the potential for insurance and employment restrictions on healthy people known to be genetically susceptible to disease, or for companies offering genetic tests to provide social networking opportunities to customers with a common genetic trait to contact each other.

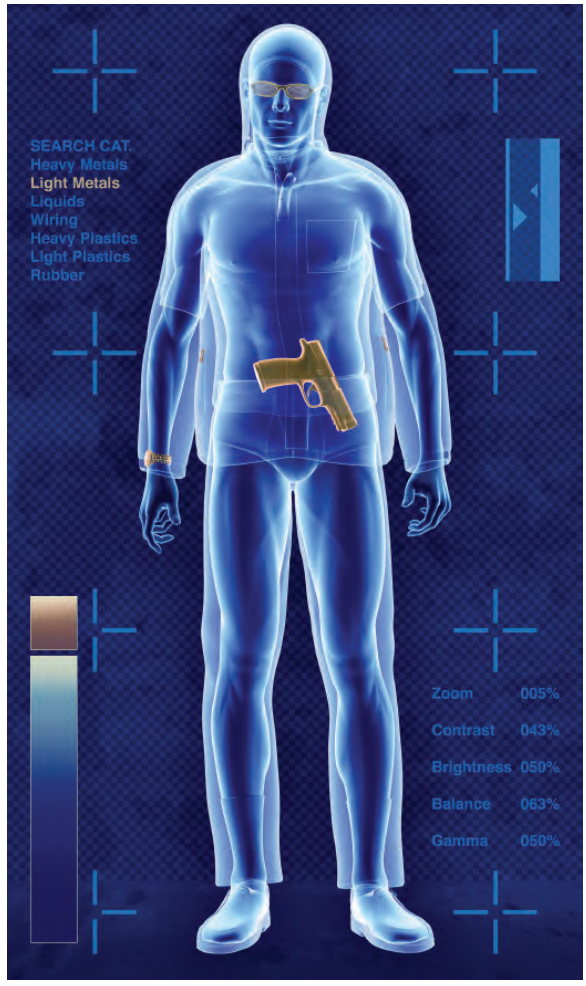
When genetic data becomes available on a massive scale, it will be a valuable resource for pharmaceuticals, hospitals and even governments. Recently, the UK human genome project called for a large number of volunteers to share their genetic data with the rest of the world for scientific purposes. As genetic information is inherited and shared within a family, participants will not only commit themselves, but to some extent also their relatives and their descendants. The privacy concerns and risks that apply to large-scale IT databases of consumer information also apply to massive databases containing genetic information, whether they are run by commercial organisations or by the scientific community.

5.3.2. Facial recognition

One of the linchpins between images of people and their personal information can be found on social media. Due to advances in facial recognition technology and the ever-increasing amount of visual information[35] uploaded to the internet, it is becoming easier to build profiles of individuals through the images that are uploaded and relate them to the information that is posted by or about them on social media and other sites.

The prevalence of smart phones and other portable devices means that facial recognition together with cloud computing services and big data analytics could be used to collate such publicly available information on individuals, so that profiling others is an option accessible to all. As advances in technology make this possible, it is important to consider what the limits on such processing should be.

5.4. Borders



The efforts to secure EU borders depend on collaboration between the member states. However,

35 In 2013, more than 350 million photos were uploaded every day on average on Facebook.

this collaboration often relies on the processing of personal information. A number of large-scale IT databases already exist to control the flow of travellers to the EU (VIS, SIS II, EURODAC) that also allow law enforcement authorities access to the information contained in those databases. The European Commission is in favour of more large-scale databases[36]; as a result, the Entry-Exit system (EES) and the Registered Traveller Programme (RTP) may soon be operational across Europe.

The EES aims to identify overstayers (those travellers who were granted a visa for a period of time but remain in the EU after their visas have expired) by registering the time and place of entry and exit of third country nationals travelling to the EU. This will allow customs officials to verify the status of a traveller without having to check the stamps in his passport, which can be a time consuming and complex process. In due time, law enforcement authorities will probably also be able to access EES data[37].

The RTP will allow frequent travellers from third countries to enter the EU using simplified border checks, subject to pre-screening and vetting. This means that travellers who submit their personal data before travelling will benefit from a faster and simpler process through border controls.

The debate on the proposals for the RTP and EES[38] continues (see section 3.4.4). Both systems will involve the collection of increasing amounts of personal data, including biometric information - fingerprints - and integration with Automated Border Controls (automated passenger checks at border crossings using new technologies under the supervision of border guards).

As demonstrated by the 2013 security incident over SIS data[39], a security breach of these large-scale IT systems could have implications for the personal data of a significant number of individuals across the EU. As more databases are created and access to the data that is held on them is granted more widely, the risk that personal information is compromised or misused also increases.

5.5. Drones

Drones, also known as remotely piloted aircraft systems (RPAS) or unmanned aerial vehicles (UAV) are aircraft that operate without an on-board pilot. Drones have predominantly been used for military applications, but there is now a proliferation of scientific and civil uses for them, in tasks too difficult or costly to carry out using existing aerial technology. Recent models of drones are more stable than ever and have autopilot capabilities, reducing the time, human involvement and cost of flying them.

Equipped with high definition cameras, drones can be used for live video streaming and real-time surveillance. The potential risk to privacy, therefore, depends partly on the type of sensors that drones carry and on the size and visibility of the aerial carrier device.

As drones are not limited to operating in outdoor public spaces, they can be highly intrusive. The control an individual may have over drone surveillance is extremely limited. Even when detected, it can be difficult to identify the operator or the purpose or technology with which the drone is equipped.

As drone technology continues to evolve, privacy implications remain a significant concern. In spite of this, there is as yet little incentive to adhere to the principle of privacy-by-design.

36 http://ec.europa.eu/commission_2010-2014/malmstrom/news/archives/2013/02/20130228_en.htm

37 http://database.statewatch.org/article.asp?aid=32381

38 http://www.dw.de/eu-smart-borders-plan-raises-big-brother-flags/a-16639437EDPS Opinion on EES and RTP

39 http://www.theregister.co.uk/2013/06/07/pirate_bay_founder_named_as_suspect_in_paneuropean_police_database_hack/

6 INFORMATION AND COMMUNICATION

Our strategic objective

Develop a creative and an effective communication strategy.

6.1. Introduction

Information and communication activities play a key role in helping to increase the awareness of the EDPS' mandate, policies and decisions both within the EU administration and the wider public. We use a range of communication tools and activities tailored to the different audiences and their varying degrees of knowledge of data protection. Regular press releases, publications, events, tweets and updates on our website are some of the activities that form part of our policy to raise the awareness of key topics.

One of the overall objectives of the EDPS strategy 2013-2014 is to build awareness of data protection as a fundamental right and a vital part of good public policy and administration for EU institutions.

To this end, in 2013, we continued in our aim to raise awareness both of the EDPS' work - legislative Opinions, prior check Opinions, data protection rights and obligations, training of EU data protection officers - and of data protection in general. Our objective is to promote a *data protection culture* within the EU institutions and bodies so that they are aware of their obligations and are accountable for compliance with data protection requirements.

In the second half of the year, the data protection reform and the revelations on mass surveillance

were the issues that dominated the headlines, and as a consequence the Supervisors and the staff devoted considerable efforts to address the issue - from media enquiries, press interviews, information requests to speeches and hearings.

Our increased visibility as an institution is confirmed by indicators such as the number of information requests received from citizens, media enquiries and interview requests, the number of subscribers to the newsletter and followers of the EDPS account on Twitter, as well as invitations to speak at conferences and website traffic. These all support the view that we are increasingly a point of reference for data protection issues at EU level.

6.2. Communication features

The EDPS communication policy is tailored to our target audience and while it is adaptable, it is in keeping with the specific features of our organisation: age, size and remit and the needs of our stakeholders.

6.2.1. Key audiences and target groups

While many organisations, including other EU institutions and bodies address EU citizens as a whole and can choose to address their audiences according to age group, profession, gender, marital status, educational background, geographic area and so forth, our direct sphere of action is more distinct.

Our supervision of EU institutions and bodies means that they are a key audience and we tailor our messages to EU staff accordingly. Other key groups include data subjects in general, EU political stakeholders and those in the data protection community.

Our communication policy does not, therefore, need to engage in mass communication. Instead, awareness of data protection issues among EU citizens in the members states depends essentially on a more indirect approach, via data protection authorities at national level, for instance.

Our communication with the general public is through a number of tools such as our website, Twitter, publications such as our newsletter and factsheets, awareness-raising events and our regularly interaction with interested parties - through study visits, for instance - and participation in public events, meetings and conferences.

6.2.2. Language policy

The EDPS strategy 2013-2014 takes into account that data protection issues are often perceived as fairly technical and obscure for non experts. Consequently, the strategy highlights that our communication work will use straightforward language to make technical issues more accessible.

In 2013, we continued to make huge strides towards our clear language goal, particularly when communicating with the general public and press. The over-riding aim has been to correct the excessive legal and technical image of data protection.

Of course, when we address more informed audiences, such as data protection specialists, more specialised language is appropriate. We recognise that different communication styles and language patterns maybe appropriate to communicate the same news to different audiences.

Our press and communication activities have been offered in at least three languages - English, French and German - since 2010 to reach the widest possible audience.

6.3. Media relations

We aim to be as accessible as possible to journalists as they provide a major channel for the public to follow our activities. Regular interaction with the media through press releases, interviews and press events help us in our endeavour to cultivate an image of a reactive and reliable partner and to promote the EDPS as an independent and authoritative point of reference for data protection at EU level.

The handling of regular media enquiries allows further contact with the media, and in 2013 we continued to update and maintain an impressive list of contacts across the media.

6.3.1. Press releases

In 2013, we issued 11 press releases. The majority of these related to our consultation work, particularly new legislative Opinions directly relevant to the general public. Among the issues covered by these

press releases were the EU data protection reform, Europol, cyber security, anti-money laundering, smart borders and eCommunications.

Our press releases are published on our website and on the Commission inter-institutional database of press releases (RAPID) in English, French and German. The press releases are distributed to our regularly updated network of journalists and interested parties.

The information in our press releases usually results in significant media coverage by both the general and specialised press. In addition, our press releases are frequently published on institutional and non-institutional websites ranging from EU institutions and bodies, to civil liberty groups, academic institutions, information technology firms and others.

6.3.2. Press interviews

In 2013, the EDPS and the Assistant EDPS gave 45 direct interviews to journalists from print, broadcast and electronic media, both European and international.

The resulting articles featured in international, national and EU press, both mainstream and specialised (IT, the EU and so on) as well as interviews on radio and television.

The interviews covered horizontal themes such as the current and upcoming challenges for privacy and data protection. They also addressed specific issues that made the headlines in 2013, including the review of the EU legal framework for data protection, lobbying in relation to this review, mass surveillance following the NSA revelations, internet security, border control, data retention and collection, big data, national DPAs and end of mandate reflections.

6.3.3. Press conferences

In 2013, we held one lunchtime press conference on 29 May, directly after the presentation of our Annual Report 2012 to the LIBE Committee of European Parliament.

The conference was an opportunity for journalists to discuss with Peter Hustinx, EDPS, and Giovanni Buttarelli, Assistant Supervisor, the implications of the EU data protection reform and in particular, the excessive lobbying of the EU legislator by industry and third countries. The conference was well-attended and the lively discussions resulted in widespread reporting of our position on the reform of the data protection rules in EU press.

6.3.4. Media enquiries

In 2013, the EDPS received some 34 written media enquiries, including requests for EDPS comments, clarifications, positions or information. Media attention was spread across many issues, most notably mass surveillance and the reform of the EU data protection rules. Other topics of interest included the EDPS itself, EURODAC, eCall, smart borders, IP tracking, whistleblowing, INDECT, data breaches, big data, cyber security, access to documents, Article 29 Working Party, Google and the iPhone fingerprint lock.

6.4. Requests for information and advice

In 2013, we dealt with 176 enquiries for information or assistance. This is an increase from 2012 (116 requests) and is a substantial number for a small organisation. The prominence of the EDPS within the data protection sphere, reinforced by our communication efforts, together with significant improvements in our website and new communication tools - factsheets and the use of Twitter - mean that we are becoming more efficient in getting our messages across.

The majority of requests for information came from individuals unaffiliated to the EU institutions asking for more information on privacy matters or assistance in dealing with problems such as the security of their personal information or the misuse of it. Other requests came from a wide range of parties, ranging from staff in the EU institutions, lawyers and law firms, private companies and industry associations, students and NGOs.

A large category of requests in 2013 concerned complaints from EU citizens about matters over which the EDPS has no competence. These complaints related mostly to alleged data protection breaches by public authorities, national or private companies and online services and technologies.

Other issues included data protection in member states, transfers of data, the excessive collection of data and slow response times of DPAs.

When complaints such as these fall outside the competence of the EDPS, we send a reply to the complainant outlining the mandate of the EDPS and advising the individual to refer to the competent national authority, usually the data protection authority of the relevant member state or where appropriate, the European Commission, or another relevant EU institution, body or agency.

6.5. Study visits

As part of our efforts to increase the awareness of data protection, we regularly welcome visits from diverse groups. In past years, such groups have often been academics and researchers or specialists in the field of European law, data protection or IT security.

In 2013, we hosted 17 groups. The majority were students or academics from the EU with others from Iceland, Norway and the U.S.A. but we were also visited by European journalists and political associations.

Most groups wanted to know more about the mandate and activities of the EDPS, but there was also much interest in the EU data protection reform, international cooperation, cloud computing, online profiling and the implications of data retention and surveillance on privacy and data protection.

6.6. Online information tools

6.6.1. Website

The website continues to be our most important communication channel and as such, it is updated on a daily basis. The various documents produced as a result of our activities (Opinions on prior checks and on proposals for EU legislation, work priorities, publications, speeches of the Supervisor and Assistant Supervisor, press releases, newsletters, event information and so on) are all available through this platform.

Since June 2013, the EDPS website is based on https protocol, so that all user communication with the site is encrypted, following good security practice.

Traffic and navigation

An analysis of our website traffic and navigation data shows that in 2013, we had approximately 136 293 new visitors to our website, compared to 83 618 in 2012 which is a ***significant increase of 63 %.*** *The total number of visits in 2013 was approximately 293 029 compared to 179 542 in 2012 which is an increase of 63.2 %.* [40]

After the homepage, the most regularly viewed pages were consultation, supervision and publications. The statistics show that most visitors access the website via a link from another site, such as the Europa portal or a national data protection authority website. Around 35 % of connections were via a direct address, a bookmark or a link in an email. Search engines links were used by only a few visitors.

6.6.2. Newsletter

The EDPS newsletter is a valuable tool for informing readers of our most recent activities and draws

40 Due to missing information for the period June to December 2013, the total figures for the year were calculated using the information for the period January to May 2013 and the evolution rate for the same period in 2012.

attention to news and updates on our website. The newsletter gives an overview of some of our recent Opinions on EU legislative proposals and on prior checks in our supervisory role that highlight particular data protection and privacy implications. It also highlights upcoming and recent conferences and other events, as well as speeches by the Supervisor and Assistant Supervisor. 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.

The format of our newsletters was introduced in October 2009 with the layout of each issue being taken care of by the Information and Communication team. In autumn 2013, we presented a new design for our newsletters following a long process with the Publications Office of the EU in Luxembourg to refresh the look of the newsletter and to speed up and professionalise the production process. We launched our new look newsletter in October 2013 and have so far received positive feedback on it.

Five issues of our newsletter were published in 2013, with an average frequency f one issue every two months (July and August are excluded). The number of subscribers rose from 1 750 at the end of 2012 to 1950 by the end of 2013. Subscribers include 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.

6.6.3. Twitter

Twitter is an online social network service that allows instant messaging in the form of microblogs. The format of the messages is the defining characteristic of Twitter because users post messages of up to 140 characters, known as tweets. It has been described as *the SMS of the internet* and has gained worldwide popularity.

On 1 June 2012, the EDPS joined the Twitter community (@EU_EDPS), our first step towards online interactive communication. Prior to this, our presence on Twitter was defined by EDPS and data protection related topics that regularly appeared in Twitter messages posted by others.

Our policy on the use of Twitter is published on our website. It reflects our step-by-step approach to maintain a contemporary information and communication tool that is manageable with limited resources. In light of this, we maintained this policy in 2013 and will review the success of our Twitter account and update our Twitter policy as appropriate in 2014.

In line with our policy, our Tweets have centred on our press releases, new Opinions, new publications, speeches and articles, videos, links to interesting articles regarding EDPS and data protection and upcoming participation in events.

By the end of 2013, we had tweeted 228 times, were following 322 other Twitter users and had 952 followers.

6.6.4. LinkedIn

LinkedIn is an online professional network, with over 225 million users worldwide. The network is geared to individuals. However, around 3 million businesses (enterprises and professional organisations) have LinkedIn company pages, with many EU institutions and data protection authorities among them.

A company page was automatically created by LinkedIn for us, when it became apparent to them from the information uploaded by users, that the EDPS is an employer. As the information contained on this page was basic and inaccurate, we took ownership of this page in December 2013 so that we could 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 2013, we had 104 followers.

The EDPS remains vigilant to the many privacy risks associated with the use of social networking services and we follow clear rules in our use of such services.

6.7. Publications

6.7.1. Annual Report

The annual report is a key publication for the EDPS. It is an overview of our work in the main operational fields of supervision, consultation, cooperation, as well as IT developments from the reporting year and also sets out the main priorities for the following year. In addition, it describes what has been achieved through external communication as well as developments in administration, budget and staff. A chapter is also dedicated to the activities of the EDPS' DPO.

Feedback suggests that the report is of particular interest to specific groups and individuals at international, European and national levels – data subjects in general and EU staff in particular, the EU institutions, data protection authorities, data protection specialists, interest groups and non-governmental organisations active in the field, journalists and anyone seeking information on the protection of personal information in the EU.

The Supervisor and Assistant Supervisor presented our 2012 Annual Report to the LIBE committee in the European Parliament on 29 May 2013.

6.7.2. Thematic publications

In 2012, we published the first of our thematic factsheets on our website, *Your personal information and the EU administration: What are your rights?* The factsheet is available in English, French and German.

In 2013, we published a further three factsheets in these languages containing information for the general public and other interested parties:

- Factsheet 2 - *Transparency in the EU administration: Your right to access documents*
- Factsheet 3 - *The EDPS: Supervising EU institutions and bodies & enforcing data protection principles*
- Factsheet 4 - *The EDPS: Keeping an eye on video-surveillance in the EU administration*

6.8. Awareness-raising events

We are keen to seize opportunities 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.

Whilst our Supervisors are the authentic voice of the EDPS, we consider that all staff are ambassadors for the organisation and thus are responsible for communicating our data protection messages when we come into contact with key audiences.

Our Supervisors are invited to numerous events in any given year, and where possible and appropriate to do so, they will accept these opportunities to disseminate our key messages.

In 2013, Peter Hustinx, EDPS, attended approximately 57 events, 50 of which he was invited to speak at. Giovanni Buttarelli, Assistant EDPS, attended approximately 42 events and spoke at 33.

While many of these events will have been data protection or privacy related, these numbers nonetheless reflect the growing awareness and interest in data protection and also in our institution as a point of reference for it.

6.8.1. Data Protection Day 2013

On 28 January 2013, 47 countries of the Council of Europe as well as European institutions, agencies and bodies celebrated the seventh 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.

This annual event was once again an opportunity for the EDPS and data protection officers from EU institutions to focus on raising awareness among EU staff and others on their data protection rights and obligations, of which the implementation within the EU administration is supervised by the EDPS.

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

In cooperation with the European Parliament, we also organised a joint conference *What will the data protection reform change for EU officials and citizens?* The conference was a huge success with standing room only remaining within minutes of the welcome address by EP Secretary-General, Klaus Welle.

Following short presentations, Peter Hustinx, Supervisor, Giovanni Buttarelli, Assistant Supervisor and Mr. Paul De Hert, Professor at the Vrije Universiteit Brussels took part in a panel discussion.

We also co-sponsored *A look inside*, an original art exhibition centred on privacy and surveillance with the Vrije Universiteit Brussel and the Privacy Commission of Belgium.

6.8.2. EU Open Day 2013

On Saturday 4 May 2013, we participated in the annual Open Day of the European institutions in Brussels which marks the anniversary of the Schuman Declaration. The EU Open Day is an excellent opportunity for us to increase general public awareness of the need to protect privacy and personal information and also of the role of the EDPS.

There was an overwhelming response to our stand in the main building of the European Parliament, due to a number of attractions we had on offer. EDPS staff worked tirelessly to answer questions on the data protection and privacy rights of EU citizens.

A drone fitted with a camera live streamed images (which were not saved) around our stand onto a TV screen. Our aim was to demonstrate the use of drones (see section 5.5) and highlight in an eye-catching way the privacy implications of new technology. We also set up two computers on our stand loaded with a web tracking application. Visitors were able to get an idea of how much of their online activity is tracked when surfing the internet and EDPS staff were on hand to answer questions and offer guidance.

Visitors could also take part in our data protection quiz as well as taking away information material.

7 ADMINISTRATION, BUDGET AND STAFF

Our strategic objective

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

Our guiding principle

We seek to be an authoritative body by developing and building the expertise and confidence of our staff to engage effectively with our stakeholders.

7.1. Introduction

In an on-going climate of economic austerity and budget consolidation, the EDPS had *to do more with less* for a second consecutive year. To make this possible, we continued our efforts towards better planning, monitoring and more efficient allocation of resources.

This context of austerity made the preparation of the draft budget for 2014 particularly difficult because it coincided with the drafting of the new Multiannual Financial Framework 2014-2020. This was a difficult forward planning exercise due to the uncertain outcome of the revision of the EU Data Protection Framework and its impact on the roles and responsibilities of the EDPS.

In 2013, we invested considerable energy and resources in further professionalising the HR function with the aim of freeing resources from purely administrative or bureaucratic tasks for more substantial HR processes. For example, SYSPER2 was successfully equipped with new modules for staff management such as NDP (Numérisation de Dossier Personnel) which allows all EDPS staff direct access to their personnel folders.

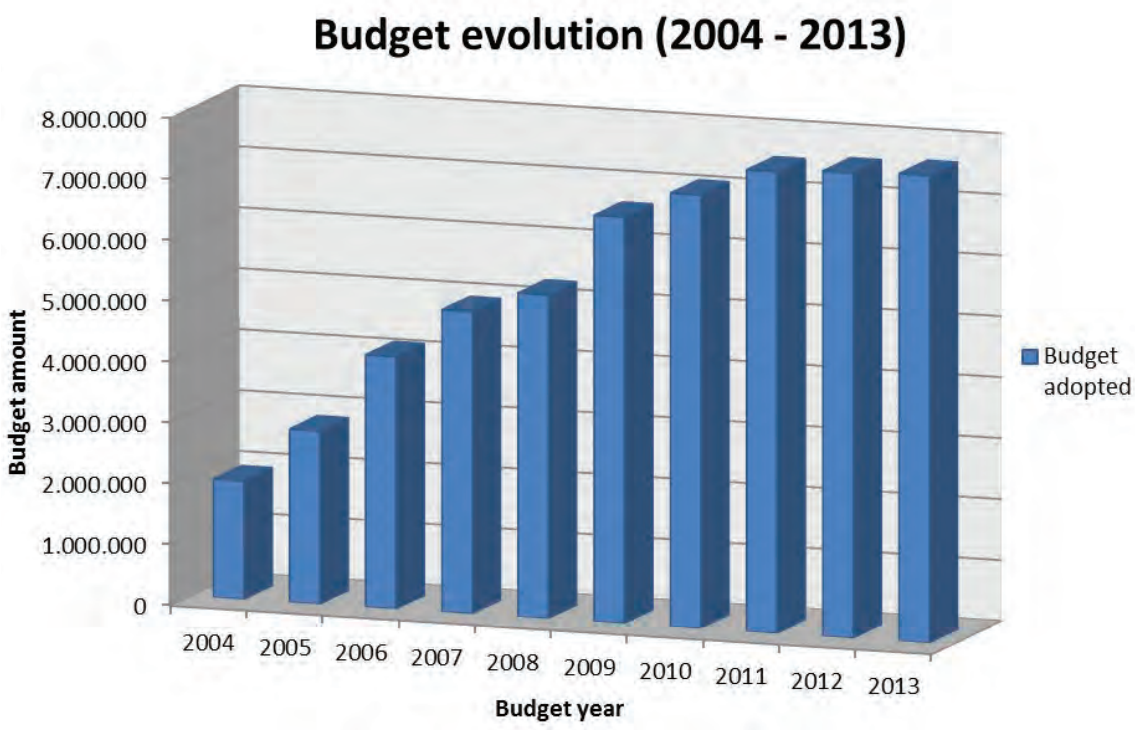
As our resources are limited, it can be difficult to balance strategic expectations with what can be achieved in reality.

7.2. Budget, finance and procurement

7.2.1. Budget

The allocated budget for the EDPS in 2013 was 7 661 409 Euro, which represents an increase of 0.49 % in the 2012 budget. This is actually a nominal reduction, taking into consideration the inflation rate of 1.9 % for 2013.

For the second year, our budget shrank during a growth phase. The EDPS budget is small in comparison to other institutions, with the result that the proportion for staff salaries represents 51 % of the total budget and our margin for manoeuvre is correspondingly limited. Nevertheless, by reducing or freezing a large majority of our credits to 0 %, we



managed to implement a policy of austerity that went beyond the 1.9 % ceiling set by the Commission; in addition to the extra credit for new salaries, the overall increase of the EDPS budget was limited to 0.49 %.

This result was made possible with a considerable effort to prioritise, a strategic redeployment of resources as well as a continuous will *to do more with less*. Quarterly reviews of the implementation of our budget have led to better implementation rates which have improved year on year: from 76.9 % in 2011, 83.2 % in 2012 to 84.7 % in 2013[41].

Due to the specificities of the EDPS budget mentioned above, it is extremely difficult to achieve an implementation rate above 85 % due mainly to unavoidable occurrences such as turnover of staff in the second half of the year that had a huge impact on the overall execution rate.

In addition, the unexpected decision by the Court of Justice of the European Union on the adjustment of salaries had a negative impact on the final implementation rate. If the salary adjustment of 2011 had been paid in 2013, the implementation rate of the 2013 budget would have increased to 87.2 %.

As a result of the policy of moderate but sustainable growth as anticipated in the Financial Perspectives for 2007-2013, we successfully completed the EDPS establishment plan with the two posts granted by the Budgetary Authority to assist in the achievement of the following core activities:

- reinforce efforts in supervision and enforcement;
- provide resources for a new IT Policy sector charged to ensure that technological developments in IT are adequately taken into account;
- contribute to the on-going discussions of the new data protection legal framework, in particular the Review of Regulation (EC) no 45/2001;
- strengthen the cooperation with the national supervisory authorities in the coordinated supervision of large scale IT-systems, with three new systems under the remit of the EDPS in 2012 and 2013;
- put in place adequate mechanisms for better planning, coordination and more efficient allocation and use of resources to be able to do more with the same or fewer resources in the future.

Looking ahead, it is possible that the on-going discussions in the Council and the Parliament about the new data protection legal framework proposed by the Commission on 25 January 2012 may result

41 In order to be consistent with the set of KPIs established to monitor the implementation of the Strategy 2013-2014 (see page 18), in 2013 the EDPS has adopted a new method of calculation for the rate of budget implementation. Under this method the current rate is based on the payment appropriations executed during 2013 as regards the budget of 2013, while the previous method included, in addition, the estimated execution of those payment appropriations carried forward to the following year.

in new roles and responsibilities for the EDPS, notably in the provision of an independent secretariat for a new European Data Protection Board which will have the task of ensuring coordination and consistency of data protection at EU level.

In order to mark the impact on resources that this reform may have upon our small institution, a new Title III has been added to our budget. However, as the negotiations between the Council and the Parliament are on-going, no additional appropriations were requested for the new Title III for the 2013 exercise.

7.2.2. Finance

There were no concerns or recommendations for the EDPS to consider in the Statement of Assurance from the European Court of Auditors for the financial year 2012 (DAS 2012). Nevertheless, within the context of sound financial management and with a view to improve the reliability and quality of our financial data:

a. the charters of tasks and responsibilities of authorising officers by delegation and sub-delegation were signed in the first half 2013;

b. an explanatory note for low value procurement procedures to be completed and attached to each purchase order or contract was adopted in January 2013;

c. a decision establishing the rules on the reimbursement for external experts hired to carry out specific tasks was adopted in July 2013.

The Commission continued to assist us in finance matters in 2013, particularly in relation to accountancy services, as the Accounting Officer of the Commission is also the Accounting Officer of the EDPS. A service level agreement for this and the use of the Commission's IT accounting system (ABAC), was signed with DG BUDG of the Commission in May 2013.

Charters for the authorising officer by delegation and by sub-delegation were prepared and signed by the EDPS Director and the head of the HRBA unit.

7.2.3. Procurement

Following the entry into force of the new Financial Regulation on 1 January 2013, an updated version of our *step-by-step procurement Guidelines for low value* contracts was adopted on 30 January 2013. However, no procurement procedures were launched in 2013.

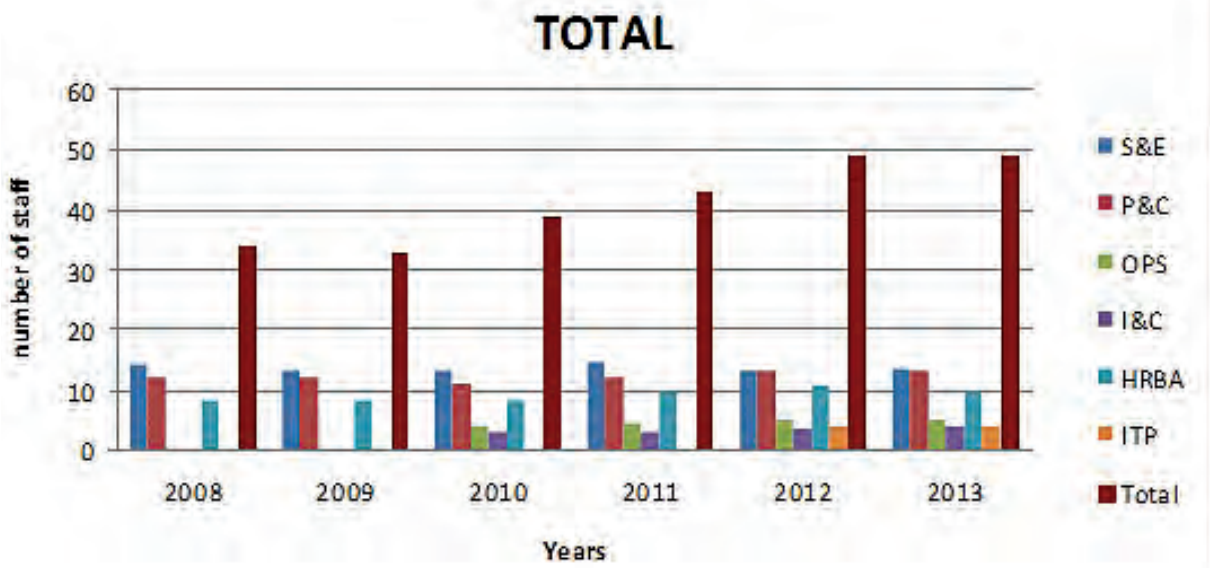
As part of our drive towards greater autonomy, we began to take part in the inter-institutional process for calls for tender. This has allowed us to make specific contracts directly with the companies to which these framework contracts have been awarded rather than rely on larger institutions acting as intermediaries to facilitate contracts on our behalf. The majority of the calls for tender of interest to us are in technical and IT related fields.

7.3. Human resources

7.3.1. Recruitment

Recruitment is one of the main activities in human resources (HR) and a strategic function for our insti-

EDPS Staff Evolution 2008-2013



tution. It involves the human resources team as well as line managers and colleagues involved in the selection panel. It is a time consuming activity but an important element in matching the right person with a vacancy as quickly as possible.

Regardless of the comparatively small size, we are bound by the same high standards of recruitment as the larger European institutions (which have staff dedicated full time to selection and recruitment activities) and the same rules as set out in the staff regulations for officials of the European Union. This implies a high degree of versatility in the job functions of our HR staff, who are responsible for a variety of responsibilities which would be dealt with by different units or directorates in the larger institutions.

In compliance with the Staff Regulations, EDPS staff are recruited as officials or as contract agents. The EDPS also recruits external staff as seconded national experts, interim staff, trainees, etc.

Officials are recruited either from other European institutions through inter-institutional transfers, or from reserve lists of laureates of European Personnel Selection Office (EPSO) general competitions. In the last four years the majority of officials specialising in data protection were recruited from a list of laureates of a data protection competition organised by EPSO on the EDPS' request. These lists were closed at the end of 2013. In view of the proposed increase in the secretariat of the future, we initiated discussions with EPSO about the possible organisation of a fresh specialist data protection competition in the future.

In the last quarter of 2013, the budgetary authority granted us two new posts for officials that have been kept on hold until 2014, following the adjustments required by the Budgetary Authority for gradual but significant cuts in the establishment plan (the number of authorised staff per institution and the related budget). These adjustments apply to all EU institutions in the framework of the new staff regulations, which entered into force on 1January 2014.

In 2013, we recruited one EU official for our Policy and Consultation team. In addition, we recruited 8 contract agents across all 4 teams, except IT policy.

Contract agents are recruited for a period that varies between a few months and 3 years in order to cover our short terms needs (maternity leave replacements, for example) or to assist with critical workloads which cannot be covered by existing staff alone.

In addition to recruitment activities related to staff turnover, this explains the stabilised growth rate in staff numbers in 2013. See the chart on the previous page.

7.3.2. Professionalising the HR function

The HR team submitted its second report on metrics, past and planned activities to the EDPS Management Board in February 2013.

The HR team has closely followed the activities of the European Commission HR programme of professionalisation, attending several seminars and master classes. The senior adviser of DG HR of the European Commission, who is responsible for this programme, surveyed all EDPS staff on engagement and our analysis of the results of this survey helped us to develop an action plan, which was adopted in December 2013. This plan should, among other things, further improve our internal communication and working conditions.

All these activities contribute to an increased professionalisation of the HR function within our compact institution.

7.3.3. Traineeship programme

In 2013, our organisation continued to invest in the traineeship programme, established in 2005. This programme offers recent university graduates the opportunity to put their academic knowledge into practice. Traineeships at the EDPS also offer practical experience in our day-to-day activities both in the operational units as well as in the Human Resources, Budget and Administration (HRBA) unit and in the Information & Communication (I&C) sector.

The programme hosts on average four trainees per session, with two five-month sessions per year (March to July and October to February). In exceptional situations and under stringent admission criteria, we may also welcome non-remunerated trainees who wish to gain experience in the framework of their studies or professional career. The admission criteria and other rules governing the traineeship programme are outlined in our traineeship decision, available on our website.

All trainees, whether remunerated or not, contribute to both theoretical and practical work and gain useful first hand experience.

7.3.4. Programme for seconded national experts

The programme for seconded national experts (SNEs) at the EDPS was established in January 2006. On average, one or two national experts from DPAs in the member states are seconded 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 2012, the secondment of one German national expert came to an end and a new national expert was recruited from the UK Data Protection Authority (ICO). As the contract of the UK expert will end in April 2014, we launched the selection procedure for a new national expert at the end of 2013.

7.3.5. Organisation chart

Other than a slight change, splitting and repositioning the functions of planning and records management, the EDPS organisation chart remained stable in 2013.

7.3.6. Working conditions

The working conditions at the EDPS (as in other EU institutions) are stipulated in the *Staff Regulations of officials and conditions of employment of other servants of the European Community*. Within this legal framework, our HR team endeavours to make conditions as attractive and flexible as possible for EDPS staff, in particular for those with family responsibilities.

The flexitime scheme is highly appreciated by staff. Most staff introduce their working hours in Sysper 2. Ten per cent use flexitime only to benefit from flexible working hours while the remainder use it not only to have flexible hours but also to recover overtime (in days or half days).

Since May 2012, our flexitime procedure has been covered by the time management module in Sysper 2; all requests and authorisations are managed through the application.

The pilot phase of our teleworking decision was prolonged to the end of June 2013 and then amended slightly. There is a choice of two teleworking schemes: structural and occasional. Structural teleworking is recurrent (maximum one day or two half days per week), while occasional teleworking is designed to cover situations where the staff member is unable to get to the office for a legitimate reason but is able to work nonetheless (maximum of twelve days per year).

In 2013, five staff members made use of structural teleworking and there were seventy requests for occasional teleworking.

7.3.7. Learning and development

Learning and development continued to grow in 2013. The importance of training has been identified in the EDPS Strategy 2013-2014 and is a key performance indicator (KPI), measuring the number of staff training days completed.

In 2013, out of a possible 277.5 training days in the training plans of our staff, 235.85 had been taken up by the end of December 2013. This corresponds to an implementation rate of 85 %.

The table below shows the number of training days completed by each team (training sessions for our new case management system (CMS) are not taken into account):

Team	Rate of implementation
S&E	**68.07 %**
P&C	**64.31 %**
ITP	**79.56 %**
OPS	**42.61 %**
I&C	**43.62 %**
HRBA	**82.25 %**
Director	**100.00 %**

The table below shows the reasons and consequence (in number of days and budget) of training that could not or was not taken up in 2013:

Reasons	Number of days	Budget
Staff leaving	18	3 025
Maternity leave	9	1 485
No training session available (or full or not suitable)	12	3 110
Person not accepted (no derogation done to the admissibility conditions)	1.5	0
Course replaced by another one	3.5 (difference between the 2 courses)	856 (difference between the 2 courses)
Foreseen course too much similar to another one already followed	3	500
Change of duration of the course (Need to cancel because of part time)	0.5	0
Course cancelled by the organisers (lack of participants)	2	600
Course cancelled by the participant (work related reason)	2	335
Total	**51.5**	**9 911**

In 2013, there was one tailor-made training course for the management team on planning and monitoring.

7.3.8. Social activities and family matters

The EDPS benefits from a cooperation agreement with the Commission to facilitate the integration of new staff, for instance by providing legal assistance in private matters (rental contracts, taxes, real estate, etc.) and by giving them the opportunity to participate in various social and networking activities.

New staff are personally welcomed by the Supervisor, the Assistant Supervisor and the Director. In addition to their mentor, newcomers also meet members of the HRBA team, who provide them with our administrative guide and other information on our specific procedures.

We continued to develop inter-institutional cooperation for childcare: the children of EDPS staff have access to the *crèches*, the European schools, after-school childcare and the outdoor childcare centres of the Commission. We also participate as an observer in the European Parliament advisory committee on prevention and protection at work, the aim of which is to improve the work environment.

In 2013, several social activities were organised together with the EDPS staff committee of the institution.

The Cloud, a social room in our new building, has been used for a number of activities, including birthday celebrations, breakfasts and a weekly

pilates class. Meetings of the staff committee also take place there.

7.4. Control functions

7.4.1. Internal control

Our internal control system, operational since 2006, manages the risk of failure to achieve business objectives. In 2012, we extended the list of actions to ensure a more efficient internal control of the processes in place. A revised decision on Internal Control Standards (ICS) was adopted in January 2013 to simplify the approach, increase ownership and strengthen their effectiveness. The tool used for monitoring the ICS implementation was thoroughly revised in line with the new ICS decision. The European Commission's Internal Audit Service (IAS) praised it as an effective tool at the Global Risk Assessment meeting that took place in 2013.

Following the EDPS decision on risk management in July 2012 (where we built on our system of assessing risks to managing them by exploring the means to overcome those risks), the first risk register was added to our Annual Management Plan (AMP) in January 2013. Following meetings with all heads of teams to identify risks at the beginning of the year, a progress report on risk management was published in July 2013.

The EDPS' Internal Control Coordinator (ICC) acknowledged the substantial efforts of all teams to implement most of the checks and controls defined in the meetings. The risks associated with heavy workloads due to over-ambitious planning and the pressure resulting from the end of the mandate of our Supervisors are mitigated by the checks and controls put in place by all teams and have benefitted the institution significantly.

Risk management is an essential element in our overall strategy of total quality management (TQM) and a training course relating to the Common Assessment Framework (CAF) was attended by our ICC in 2013 as the part of the TQM strategy. Accompanied by a list of criteria, a self-assessment questionnaire which analyses all the operational and administrative processes of an organisation is to be completed. The CAF will give us a complete overview and highlight any processes that need to be refined.

Taking into account our annual activity report and the Statement of Assurance signed by the authorising officer by delegation, we believe that the internal control systems we have in place offer reasonable assurance of the legality and regularity of operations for which we are responsible.

7.4.2. Internal audit

The Internal Auditor of the Commission, the head of the IAS, is also the internal auditor of the EDPS.

In October 2013, the IAS issued the Annual Internal Audit Report (ARIA - Article 99(3) of the Financial Regulation) for 2012, which summarised the internal audit activity in 2012 at the EDPS.

The IAS intention to conduct an HR audit in 2013, which did not materialise, triggered an internal review within the HR function, leading to tangible improvements.

A follow up audit visit by the IAS in June 2013 concluded that:

- Two important recommendations stemming from the IAS Limited Review of Internal Control Standards had been adequately implemented (controls in the mission procedure and supervision of staff files);
- One desirable recommendation issued in the IAS audit on Supervision and Enforcement had been adequately implemented;
- Six recommendations issued in the IAS audit on Supervision and Enforcement were not ready for review at the time of the follow-up visit and were therefore not assessed. However, in July 2013, the new version of our manual dealing with prior checks included some modifications in response to these recommendations.

One pending recommendation relates to a case filing system. As described in section 7.6.2, the EDPS case management system became operational in October 2013, therefore it is reasonable to expect that this recommendation will be closed in the near future.

In addition to this follow-up audit, the IAS visited the EDPS in September-October 2013 for a global risk assessment of our activities. The overall conclusion of the IAS was that it was evident that we had made considerable efforts which had resulted in substantial improvements since the last assessment in 2011. Most of the processes previously considered as insufficiently mature or under control have improved and those few still considered insufficiently mature are being addressed (work in progress).

7.4.3. External audit

As an EU institution for the purposes of the financial Regulation, the EDPS is audited by the Court of Auditors. Pursuant to Article 287 of the Treaty on the Functioning of the European Union, the Court audits our revenue and expenditure annually to provide a statement of assurance as to the reliability of our accounts and the legality and regularity of the underlying transactions. This takes place in the framework of the so-called *discharge exercise* with audit questions and interviews.

For the discharge of the year 2012, the questions posed by the Court were answered satisfactorily by the EDPS. In June 2013, for the second consecutive year, a letter to the EDPS from the Court stated: "*no observations resulted for the audit work carried out*".

The Court of Auditors (Article 162 of the Financial Regulation) stated that it did not identify any significant weakness in the areas it audited. The measures implemented (social allowances) as a result of its audit in 2009 were effective. We took note of the Court's analysis and will continue to improve our systems for timely monitoring and control.

On 22 January 2013, the EDPS Director attended the discharge meeting at the Budgetary Control Committee at the European Parliament and responded to the questions posed by the members of the Committee. The European Parliament granted the EDPS discharge for the implementation of our budget for financial year 2011.

7.5. Infrastructure

The offices of the EDPS are located in one of the buildings of the European Parliament, and we were pleased to move to our new premises on Rue Montoyer 30 in Brussels at the beginning of October 2012. The rent and other associated costs are borne by our institution and the institution continues to manage its furniture inventory independently. DG ITEC of the Parliament supports us with IT and infrastructure on the basis of a mutually agreed IT flat rate charge.

In 2013, we completed a number of decoration tasks in our new premises, including the improvement of the large meeting room on the ground floor used to hold workshops and seminars and the acquisition and installation of a video-conference system has allowed us to participate in many external meetings at locations further away without leaving the premises, with the corresponding savings in travel and accommodation costs.

The institution continues to manage its furniture inventory independently and as a result of a flat rate agreement with the Parliament, the IT inventory is managed by DG ITEC.

7.6. Administrative environment

7.6.1. Administrative assistance and inter-institutional cooperation

The EDPS benefits from inter-institutional cooperation in many areas by virtue of an agreement concluded in 2004 by the Secretaries General of the Commission, the Parliament and the Council, which was extended in 2006 (for a three-year period) and in 2010 (for a two-year period) with the Commission and the Parliament. An extension of the agreement for two years was concluded by the Secretaries General of the Commission and the Parliament and the EDPS Director in December 2011.

In 2012, in view of our imminent move to new offices, the European Parliament suggested a revision of the General Administrative Agreement with the EDPS, including the annexes on infrastructure, security, IT, etc. with a view to better reflect the needs and obligations of both parties, as well as to simplify and harmonise those texts. Technical aspects of the new administrative agreement were concluded in 2012 and it was officially signed in July 2013. This administrative cooperation is vital for us as it increases efficiency and allows for economies of scale.

Further to the move to our new premises, we will put in place a new business continuity plan in early 2013, in close cooperation with the European Parliament.

A new security decision has been drafted and will be adopted in the early 2014.

In 2013, we continued our close inter-institutional cooperation with various Commission Directorates-General (Personnel and Administration, Budget, Internal Audit Service, Education and Culture), the Paymaster's Office (PMO), the European Administrative School (EAS), the Translation Centre for the Bodies of the European Union. This cooperation takes place by means of service level agreements, which are updated regularly.

We also continued to participate in the inter-institutional calls for tenders, thus increasing efficiency in many administrative areas and making progress towards greater autonomy.

The EDPS is a member of the various inter-institutional committees and working groups, including the Collège des Chefs d'administration, *Comité de Gestion Assurances maladies, Comité de Préparation pour les Questions Statutaires, Comité du Statut, the Interinstitutional* Working Party/EAS, EPSO management board, EPSO working group, *Commission paritaire commune and Comité de préparation pour les affaires sociales.*

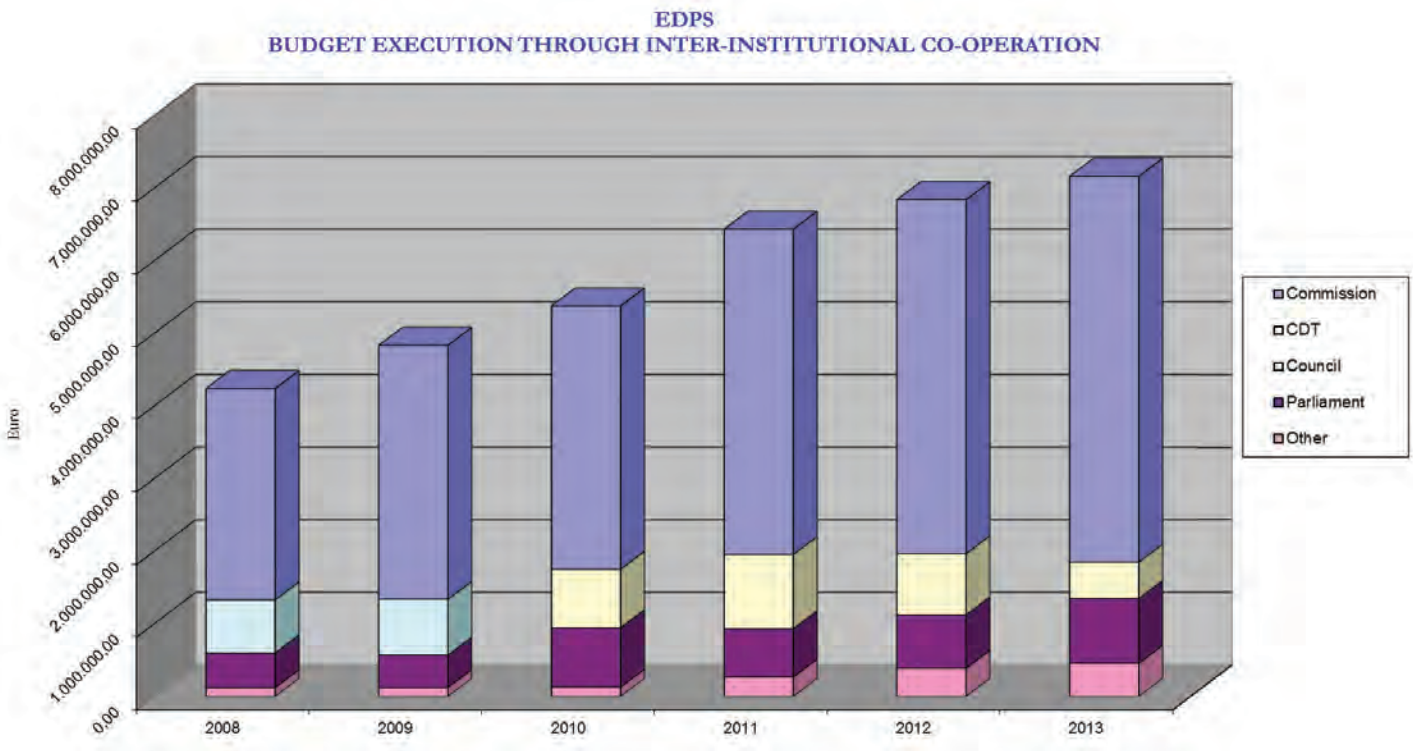
7.6.2. Document management

Our new case management system (CMS) became operational in October 2013. The system was selected following an evaluation of several products on the market and a thorough analysis of EDPS requirements, including functionalities, operations, economic aspects, security and data protection necessities. As well as commercial negotiations and functional customisation, we assessed the security management systems of suppliers and arranged security and data protection details in the contracts and service level agreements.

In the course of 2013, the entire repository of EDPS cases was successfully migrated to the CMS and operations were able to continue without interruption. Additional features will gradually be integrated into the system in due course.

Some organisational changes were made to support the launch of the CMS. Our IT Policy team is responsible for CMS operations, security and project management and so a position of Records Manager/Archivist was created within the team with primary responsibility for the functionality of the system and for the business processes supported by it. The position also incorporates the function of CMS business administrator and second level in-house support.

First level support is provided by a member of each team, nominated super-user. These super-users receive specific training and coaching so that they can help colleagues with issues that have not been addressed in the CMS induction training. The super-users give feedback to the CMS records manager about the functioning of the system and help to identify potential changes.



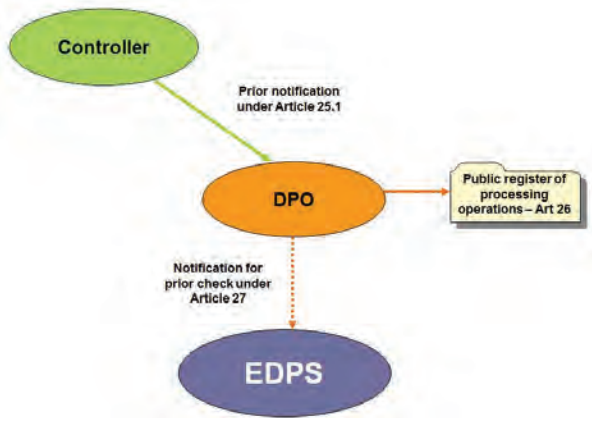
8 EDPS DATA PROTECTION OFFICER

8.1. The DPO at the EDPS

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

To strengthen this independence and consolidate her expertise, the DPO is a Certified Information Privacy Professional/Europe (CIPP/E) and will seek further certification in 2014 as Certified Information Privacy Manager (CIPM).

Notification of processing operations



8.2. The Register of processing operations

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

Following the revision of all notifications for processing operations within the EDPS in 2011 - when the conditions of a processing operation change and have consequences for personal data, the notification for this processing should be revised - and the update of the inventory (which lists all the relevant processing operations of the institution, the team in charge of the process and the date of the notification) and its implementation in 2012, 2013 was dedicated to the implementation of the inventory. There were 4 new notifications and 4 revisions of existing notifications.

As a result, 97.7 % of the inventory has been notified and implemented.

Following EDPS Guidelines, the DPO took care of the notifications submitted to the EDPS under Article 27.2 of Regulation 45/2001. However, very few notifications were subject to this provision in 2013.

> Article 27(2) of the Regulation contains a non-exhaustive list of processing operations that are likely to present specific risks to the rights and freedoms of data subjects. These are subject to prior checking by the EDPS (Article 27(1))

The DPO's main objective for 2014 is to deal with the revision of all notifications for HR procedures that relate to the implementation of the new staff regulations. Procedures relating to administrative

inquiries, disciplinary procedures and anti-harassment procedures will also be notified once they have been approved in the course of 2014.

8.3. EDPS 2013 Survey on the status of DPOs

In June 2013, the EDPS launched a questionnaire on the status of DPOs to monitor the compliance of EU institutions and bodies with Article 24 of Regulation 45/2001. In July, the EDPS Director replied to the survey giving a complete overview of the status and evolution of the DPO function within the EDPS itself.

The information provided relates to the inventory of the processing operations, the register established under Article 26, data protection training given to staff, contractual clauses for processors, involvement of the DPO in designing new processing operations and transfers to recipients not subject to national provisions implementing Directive 95/46.

8.4. Information and raising awareness

From left to right: Peter Hustinx, EDPS; Sylvie Picard, EDPS DPO; Giovanni Buttarelli, Assistant EDPS

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 (see also section 2.7.3). The website 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 took part in the DPO network meeting in Lisbon in March 2013 and hosted the DPO network meeting in Brussels in November. These meetings represent a unique opportunity to network, discuss common concerns and share best practice.

The organisation of the DPO meeting in Brussels was a worthwhile challenge which allowed the DPO to reinforce her network and to ensure that issues important to DPOs were discussed and then presented to the EDPS Supervisors on the second day of the meeting.

The interesting relationship between Regulation 45/2001 on data protection and Regulation 1049/2001 on public access to documents was discussed during the workshops. In particular, the focus was on issues such as:

1. access to records containing the names of people and details of their status (officials in active service /inactive/AD/AST staff / external staff);
2. access to records containing other types of personal data (e.g. evaluation or personnel status);
3. the necessity of the transfer and the possible prejudice to the data subject's legitimate interests under Article 8 of Regulation 45/2001;
4. access to large amounts of data or documents and the principle of reasonable effort;
5. the role of consent and information in the process of access to documents.

The workshops at the meeting were an opportunity for all the DPOs to share their practical experience on this topic.

The Brussels meeting was the last DPO meeting to be attended by Peter Hustinx, who has headed the network for the last 10 years, before the end of his mandate as EDPS. An informal farewell reception allowed DPOs to share their impressions and anecdotes with him.

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 relevant information (according to Articles 11 and 12 of Regulation 45/2001) about EDPS processing operations, allowing all staff to 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 staff with our data protection mission and values.

9 MAIN OBJECTIVES FOR 2014

The following objectives have been selected for 2014 within the overall Strategy for 2013-2014. The results will be reported in 2015.

9.1. Supervision and enforcement

We will continue to promote the principle of accountability as proposed among the changes to the data protection framework. This means that the EU administration will have to take all the measures necessary to ensure compliance with the data protection Regulation and will have to keep documentation that demonstrates their compliance.

- **Guidance and Training**

DPOs and DPCs are essential keys to being truly accountable. We will therefore continue to develop training and guidance for DPOs and DPCs and continue to foster close contacts with the DPOs and the DPO Network.

In this regard, we intend to organise training activities for new DPOs, to organise a workshop on data

subject rights and to adopt guidelines on topics such as declaration of interests, transfers and eCommunication. We also plan to update existing guidelines in the light of new developments. As part of our plan to support DPOs we will continue in our work on the EIPA certification programme for DPOs.

- **Visits**

Within the EU administration, the commitment of management and the awareness of the persons processing data are essential conditions to the success of ensuring compliance with data protection. We will therefore continue to invest resources to raise awareness at all levels and to engaging the commitment of management, primarily through visits.

- **Closer dialogue with EU institutions**

Ensuring that data protection rules are adequately respected within the constraints of the EU administration is a permanent challenge in our supervision work. We will therefore continue to engage in dialogue with data controllers, but also improve the language of our Opinions in order to promote a pragmatic and practical application of the Regulation. We will also endeavour to improve the format of our Opinions so as to make the content as accessible as possible.

- **Inspections**

Inspections will continue to be an important element of the EDPS Compliance and Enforcement Policy, based on criteria set in our Inspection Policy adopted in 2013.

- **Follow up of our Opinions and Decisions**

In recent years there has been a huge increase in the number of prior check Opinions, due to the June 2013 deadline for so called *ex-post* prior checks. The challenge for 2014 is to ensure that the recommendations made in these Opinions are effectively followed up. This will be the case for prior checks, as well as for complaints, consultations on administrative decisions, inspections and visits.

9.2. Policy and consultation

The main objective of our advisory role is to ensure that the EU legislator is aware of data protection requirements, integrates data protection measures in new legislation and sets forth actions to achieve this objective.

We will need to fulfil our increasing role in the legislative procedure and extend timely and authoritative advice with increasingly limited resources. In light of this, our inventory has been prepared by selecting issues of strategic importance that will be the cornerstones of our consultation work for 2014 (the inventory and accompanying note are published on our website).

- **New legal framework for data protection**

We will continue to interact with all relevant actors in the on-going legislative procedure for a new legal framework, as well as with stakeholders and interested parties at all levels in order to achieve the goal of a speedy adoption of the legislative package.

- **Rebuilding trust in global data flows in the aftermath of PRISM**

We will closely follow developments as the *PRISM* story *continues to unfold* and provide input to the initiatives taken by the EU institutions, in particular, the Commission, in the context of rebuilding trust in global data flows.

- **Initiatives to bolster economic growth and the Digital Agenda**

Most of the work planned by the Commission in the area of the information society and new technologies for 2014 is carried over from 2013. Particular emphasis will be given to the objective of bolstering economic growth in the EU. Some of the planned initiatives are likely to have significant data protection relevance.

- **Further developing the Area of Freedom, Security and Justice**

In 2014, the programme for the Area of Freedom, Security and Justice adopted in Stockolm in 2010 will be concluded. A new set of strategic guidelines and a multi-annual roadmap will be adopted, with some policies initialled for 2013 to be carried over.

- **Financial sector reforms**

Since the outbreak of the economic crisis, the Commission has undertaken a comprehensive overhaul of the financial regulation and its supervision. In 2013, we paid close attention to developments in

financial legislation. Apart for the envisaged *New approach to business failure and insolvency*, on which we may issue a comment or an Opinion, the majority of measures planned for 2014 are items carried over from 2013.

- **Combatting Tax fraud and banking secrecy**

Following the trend of 2013, initiatives developed at EU level to combat tax fraud and banking secrecy are expected to have data protection significance. Apart from the EU legal framework on VAT, fiscal policies remain outside the competences of the EU. Nevertheless, the EU is increasingly supporting, coordinating or complementing the actions taken by member states on administrative cooperation in the fiscal field, thus exercising the competence conferred on it by article 6 TFEU.

- **Other initiatives**

As part of our strategy to promote a data protection culture in EU institutions and bodies and to integrate respect for data protection principles in EU legislation and policies, including in areas such as competition, we may decide to issue advice on our own initiative with a view to contributing to debates on legal and societal developments that may have a major impact on the protection of personal data. In issuing these *preliminary* Opinions, we hope to stimulate an informed dialogue on these important issues which could help shape a full Opinion and recommendations thereafter.

9.3. Cooperation

We will continue to pay particular attention to fulfilling the 2013-2014 Strategy concerning cooperation with other data protection authorities, both in the field of coordinated supervision and in other important contexts. We will also continue to engage with relevant developments in international organisations.

- **Coordinated supervision**

We will continue in our supporting role in the coordinated supervision of EURODAC, CIS and VIS, in close cooperation with the data protection authorities of the member states and further develop our role in the context of the second generation Schengen Information System. In 2014, the first steps in coordinated supervision are to be expected also in relation to the Internal Market Information System.

- **Article 29 Working Party**

We will continue to actively contribute to the activities and the further development of the Article 29 Working Party, ensuring consistency and synergy between it and our own tasks in line with our respective priorities. We will also maintain our good bilateral relationships with national DPAs. As rapporteur for some specific dossiers, we will continue to steer and prepare the adoption of Working Party Opinions.

- **International organisations**

International organisations, such as the Council of Europe and the OECD, play an important role in standard setting and policy development in different areas, including data protection and related subjects. Most international organisations are, at the same time, not subject to data protection legislation in their host countries, but not all of them have their own appropriate rules for data protection in place. We will therefore continue to reach out to international organisations, either to engage with their work in standard setting and policy development, or to involve them in workshops aimed at raising awareness and exchanging good practices.

9.4. IT Policy

Monitoring developments in information technology which impact data protection and the related discussion on technology policy and relevant business developments, will help us to take technical elements better into account in our supervision activities and in our comments on EU policy initiatives. Our effectiveness in this area will benefit from close cooperation with other data protection authorities and external experts.

We will also continue to raise awareness of the needs and methodologies for assessing the risks of processing personal data in the EU institutions. In cooperation with experts both within and outside of the institutions, we will work on highlighting the range of tools and approaches that are available to select the appropriate technical and organisational safeguards to manage these risks.

Together with the relevant stakeholders in EU and national administrations and national data protection authorities, we will also continue to contribute to specific initiatives to assess and ensure the security of specific EU IT systems.

- **Guidelines for EU institutions**

Following our exchanges in 2013 with IT managers, security experts, web masters and others in the EU

Institutions and bodies, we will finalise our guidelines on legal requirements and technical measures for the protection of personal data processed through the EU websites with mobile devices and in cloud computing environments. These guidelines will also form the basis for developing systematic and regular supervision methods and tools for these areas.

- **Privacy aware internet development**

Together with other data protection authorities, we will work on improving the communication between data protection experts and developer communities, through dedicated workshops, conferences and working groups, to build a better understanding of mutual needs and develop practical ways to implement data protection and privacy requirements in new protocols, tools, components, applications and services.

In this context, we will also seek ways to ensure that more attention is given to privacy and data protection in the education of new engineers and developers. We also aim to provide advice to research agencies on supporting privacy friendly technological development.

- **IT infrastructure**

For our own IT needs, we will continue to increase efficiency and ensure that it complies with all requirements regarding data protection and security. We will further improve our internal procedures and the cooperation with our service providers.

We will also ensure that the continuous learning programs for EDPS staff take proper account of IT related elements.

9.5. Other fields

Information and communication

In line with our Strategy 2013-2014, we will continue to raise awareness of data protection within the EU administration, but also to inform individuals of their fundamental rights to privacy and data protection. To do this effectively, our efforts to increase the visibility of the EDPS as experts in data protection, including in the press and the wider public, will garner both public confidence and the commitment of the EU institutions.

Our communication activities in 2014 will include:

- updating our website and developing a section for our IT policy observations;
- the review and update of existing information and communication tools (publications, website etc.) in view of the transition into the new EDPS mandate;
- continuing 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

2014 is likely to mark the beginning of a third EDPS mandate. In the ten years since its foundation, the EDPS has matured as an institution. We are no longer confronted with the challenges of its consolidation, but rather with issues of organisational development, quality management, strategic planning and allocation of resources and retention and motivation of staff.

The entry into force of the new Staff Regulations in January 2014 will trigger the update of many implementing measures dealing with a whole range of HR issues (appraisal, leave management, working conditions, etc.). This is an enormous administrative task and requires careful planning, consultation of the EDPS staff committee and proactive communication with all staff.

The new mandate of the EDPS is also likely to result in a heavy workload for the HRBA unit, not only because new members need to be fully acquainted with the demanding requirements of our small institution but also to manage and implement any consequential changes.

We will continue working on HR activities which were started in 2013 (such as a more strategic Learning and Development Policy and the review of the Code of Conduct) while also pursuing new activities such as improvements in recruitment procedures.

The existing HR and administration teams will be merged to increase the HR capacity of the organisation.

As in previous years, the individuals working in the EDPS will continue to be our priority. We will endeavour to procure the best possible working conditions for them within the limits of the Staff Regulations, so that the EDPS continues to be perceived as an ideal workplace, with highly motivated and engaged staff.

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.[36]

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, which is now legally binding, 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 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) thereof 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,

[36] 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 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.

The duty to cooperate with national supervisory authorities and supervisory bodies in the former 'third pillar" has a similar 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 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

ORGANISATION	NAME	E-MAIL
European Parliament (EP)	Secondo SABBIONI	Data-Protection@europarl.europa.eu
Council of the European Union (Consilium)	Carmen LOPEZ RUIZ	Data.Protection@consilium.europa.eu
European Commission (EC)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Court of Justice of the European Union (CURIA)	Valerio Agostino PLACCO	Dataprotectionofficer@curia.europa.eu
European Court of Auditors (ECA)	Johan VAN DAMME	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	Dataprotectionofficer@eib.org
European External Action Service (EEAS)	Carine CLAEYS	Ingrid.HVASS@eeas.europa.eu Carine.CLAEYS@eeas.europa.eu
European Ombudsman	Christina KARAKOSTA (acting DPO) Rosita AGNEW	DPO-euro-ombudsman@ombudsman.europa.eu
European Data Protection Supervisor (EDPS)	Sylvie PICARD	Sylvie.picard@edps.europa.eu
European Central Bank (ECB)	Frederik MALFRÈRE	DPO@ecb.int
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)	Gregor SCHNEIDER	DataProtectionOfficer@oami.europa.eu
European Union Fundamental Rights Agency (FRA)	Nikolaos FIKATAS	Nikolaos.Fikatas@fra.europa.eu
European Medicines Agency (EMEA)	Alessandro SPINA	Data.Protection@emea.europa.eu
Community Plant Variety Office (CPVO)	Véronique DOREAU	Doreau@cpvo.europa.eu
European Training Foundation (ETF)	Tiziana CICCARONE	Tiziana.Ciccarone@etf.europa.eu
European Network and Information Security Agency (ENISA)	Ulrike LECHNER	Dataprotection@enisa.europa.eu
European Foundation for the Improvement of Living and Working Conditions (Eurofound)	Markus GRIMMEISEN	mgr@eurofound.europa.eu

>>>

ORGANISATION	NAME	E-MAIL
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	Ignacio Vázquez MOLINÍ	Ignacio.Vazquez-Molini@emcdda.europa.eu
European Food Safety Authority (EFSA)	Claus RÉUNIS	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.Bustamante@cedefop.europa.eu
Education, Audiovisual and Culture Executive Agency (EACEA)	Hubert MONET	eacea-data-protection@ec.europa.eu
European Agency for Safety and Health at Work (OSHA)	Emmanuelle BRUN	brun@osha.europa.eu
Community Fisheries Control Agency (CFCA)	Rieke ARNDT	cfca-dpo@cfca.europa.eu
European Union Satellite Center (EUSC)	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
Executive Agency for Health and Consumers (EAHC)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
European Centre for Disease Prevention and Control (ECDC)	Rebecca TROTT	Rebecca.trott@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 Aviation Safety Agency (EASA)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Executive Agency for Competitiveness and Innovation (eaci)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Trans-European Transport Network Executive Agency (TEN-T EA)	Caroline MAION (acting DPO)	inea-dpo@ec.europa.eu caroline.maion@ec.europa.eu
European Banking Authority (EBA)	Joseph MIFSUD	Joseph.MIFSUD@eba.europa.eu
European Chemicals Agency (ECHA)	Bo BALDUYCK	data-protection-officer@echa.europa.eu

>>>

ORGANISATION	NAME	E-MAIL
European Research Council Executive Agency (ERCEA)	Nadine KOLLOCZEK	Nadine.Kolloczek@ec.europa.eu
Research Executive Agency (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu
European Systemic Risk Board (ESRB)	Frederik MALFRÈRE	DPO@ecb.int
Fusion for Energy	Angela BARDENEWER-RATING	Angela.Bardenhewer@f4e.europa.eu
SESAR Joint Undertaking	Daniella PAVKOVIC	Daniella.Pavkovic@sesarju.eu
ARTEMIS Joint Undertaking	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Clean Sky Joint Undertaking	Bruno MASTANTUONO	Bruno.Mastantuono@cleansky.eu
Innovative Medecines Initiative (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Fuel Cells & Hydrogen Joint Undertaking	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu
European Insurance and Occupations Pensions Authority (EIOPA)	Catherine COUCKE	catherine.coucke@eiopa.europa.eu
Collège européen de police (CEPOL)	Leelo KILG-THORNLEY	leelo.kilg-thornley@cepol.europa.eu
European Institute of Innovation and Technology (EIT)	Roberta MAGGIO	roberta.maggio@eit.europa.eu
European Defence Agency (EDA)	Gabriele BORLA	alain-pierre.louis@eda.europa.eu
ENIAC Joint Undertaking	Marc JEUNIAUX	Marc.Jeuniaux@eniac.europa.eu
Body of European Regulators for Electronic Communications (BEREC)	Michele Marco CHIODI	Michele-Marco.CHIODI@berec.europa.eu
Agency for the Cooperation of Energy Regulators (ACER)	Paul MARTINET	Paul.MARTINET@acer.europa.eu
European Asylum Support Office (EASO)	Paula McCLURE	paula-mello.mcclure@ext.ec.europa.eu
European Union Institute for Security Studies (EUISS	Nikolaos CHATZIMICHALAKIS	nikolaos.chatzimichalakis@iss.europa.eu
eu-LISA	Luca ZAMPAGLIONE	Luca.ZAMPAGLIONE@ext.ec.europa.eu

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

Leave and flexitime management - IMI

Opinion of 20 December 2013 on the notification for prior-checking from the Data Protection Officer of the Innovative Medicines Initiative in the field of leave and flexitime management (Case 2013-0463)

Public procurement - OHIM

Opinion of 20 December 2013 on the notification for prior checking concerning public procurement, Office of Harmonisation in the Internal Market (Case 2013-0668)

Enquête anonyme ciblant le personnel du Parlement Européen ayant un handicap - PE

Avis du 18 décembre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Parlement Européen à propos du dossier 'Enquête anonyme ciblant le personnel du Parlement Européen ayant un handicap' (Dossier 2013-0656)

Application and granting of leave - BEREC

Opinion of 18 December 2013 on the notification for prior checking from the Data Protection Officer of the BEREC Office concerning the application and granting of all kind of leave (including special leave) (Case 2013-0405)

Public procurement - ECHA

Opinion of 18 December 2013 on prior checking notification concerning public procurement (Case 2013-0010)

Staff evaluation - EIT

Opinion of 16 December 2013 on a notification for prior-checking regarding staff evaluation for the probationary period at the European Institute of Innovation and Technology (EIT) (Case 2013-0813)

Attestation procedure - OHIM

Opinion of 16 December 2013 on a notification for prior-checking regarding OHIM's attestation procedure (ex-C and ex-D categories) (Case 2013-0797)

Ability to work in a third language - Court of Justice

Opinion of 10 December 2013 on the notification for prior checking received from the Data Protection Officer of the Court of Justice of the European Union regarding the 'ability to work in a third language' (Case 2013-0771)

Staff appraisals and probationary reports - SESAR

Opinion of 2 December 2013 on the notifications for prior checking received from the Data Protection Officer of the SESAR Joint Undertaking regarding the Joint Undertaking's staff appraisal procedures and its procedure for probationary reports (Cases 2013-0699 and 2013-0700)

Leave management - EDA

Opinion of 21 November 2013 on the notification for prior checking from the Data Protection Officer of the European Defence Agency in the area of leave management (Case 2013-0741)

Staff and trainee selection, recruitment and management - TEN-T EA

Opinion of 21 November 2013 on the notification for prior checking concerning internal mobility (Case 2013-0871) and the selection, recruitment and management of interim staff (2013-0871), of blue book trainees (2013-0872) and of atypical trainees (2013-0873) at the Trans-European Transport Network Executive Agency (TEN-T EA).

Anti-harassment procedures and the selection of confidential counsellors - F4E

Opinion of 21 November 2013 on the notification for prior checking concerning the anti-harassment procedures and the selection of confidential counsellors at F4E (Case 2013-0326)

Grants for university based interpreting courses - EP

Opinion of the 21 November 2013 on the notification for prior-checking concerning processing operations involving personal data in the context of the procedure for the awarding of 'grants for university based interpreting courses' (Case 2013-0653)

Public Procurement – FRA

Opinion of 19 November 2013 on the notification for prior checking concerning the processing of personal data in the context of public procurement at the Fundamental Rights Agency (Case 2013-0660)

Leave and time management - ECHA

Opinion of 14 November 2013 on the notification for prior checking from the Data Protection Officer of the European Chemicals Agency on leave and time management (Case 2013-0345)

Time and absence management - ECDC

Opinion of 14 November 2013 on the notification for prior checking from the Data Protection Officer of the European Centre for Disease Prevention and Control Agency in the field of time and absence management (Case 2013-0362)

Selection of the Chair of the Supervisory Board - Parliament

Opinion of 14 November 2013 on the notification for prior-checking concerning the selection of the Chair of the Supervisory Board (Case 2013-1090)

Selection and recruitment - EDA

Opinion of 5 November 2013 on the notification for prio-checking concerning 'EDA Selection and Recruitment procedure for Temporary Agents (TA), Contract Agents (CA), Seconded National Experts (SNE) and Interns' at the European Defence Agency (Case 2013-0743)

Staff appraisal procedures - EEA

Opinion of 5 November 2013 on the notification for prior-checking recieved from the Data Protection Officer of the European Environment Agency (EEA) concerning the EEA's staff appraisal procedures (Case 2013-0791)

Public Procurement & Grants - EFSA

Opinion of 31 October 2013 on the notification for prior checking concerning the processing of personal data in the context of public procurement and grant procedures at the European Food Safety Authority (Case 2012-0666)

Public Procurement – EASA

Opinion of 31 October 2013 on the notification for prior checking concerning the processing of personal data in the context of public procurement and related contract management at the European Aviation Safety Agency (Case 2012-0647)

Leave management - Court of Justice

Opinion of 29 October 2013 on notifications for prior checking from the Data Protection Officer (DPO) of the Court of Justice of the European Union concerning records relating to the management of special leave and maternity leave (Case 2013-0189), the management of working time organisation (part time) (Case 2013-0223), the management of parental leave and family leave (Case 2013-0267) and the management of leave on personal grounds of the staff of the Court of Justice (Case 2013-0337)

Leave management - CEPOL

Opinion of 29 October 2013 on the notification for prior checking from the Data Protection Officer of the European Police College on the management of sick leave, annual leave and special leave and on the management of working hours and flexitime (Case 2013-0315)

Whistleblowing Procedures - TEN-T EA

Opinion of 28 October 2013 on a notification for Prior Checking received from the Data Protection Officer of the Trans-European Transport Network Executive Agency (TEN-T EA) on a Whistleblowing Procedures (Case 2013-0916)

Public Procurement – ERCEA

Opinion of 21 October 2013 on the notification for prior checking concerning the processing of personal data in the context of public procurement at the European Research Council Executive Agency (Case 2012-0921)

Recruitment procedure - EFCA

Opinion of 21 October 2013 on the notification for prior-checking concerning the processing of personal data in the context of the recruitment procedure for temporary agents, contract agents and seconded national experts (Case 2013-0735) and service contracts for trainees under the agreement for educational cooperation with the University of Vigo (Case 2013-0736) at European Fisheries Control Agency

Public Procurement & Grants – ECDC

Opinion of 17 October 2013 on the notification for prior checking concerning the processing of personal data in the context of public procurement and grant procedures at the European Centre for Disease Prevention and Control (Case 2012-1089)

Staff assessment procedure - EDA

Opinion of 16 October 2013 on the notification for prior checking from the Data Protection Officer of the European Defence Agency (EDA) concerning the 'staff assessment procedure' (Case 2013-0744)

Processing of personal data in the context of internships - FRA

Opinion of 16 October 2013 on the notification for prior-checking concerning the processing of personal data in the context of internships at the European Union Agency for Fundamental Rights (Case 2013-0654)

Probationary period reports for temporary and contract agents - EEA

Opinion of 14 October 2013 on a notification for prior checking received from the Data Protection Officer of the European Environment Agency (EEA) on the processing operations related to the EEA's probationary period reports for temporary and contract agents (Case 2013-0787)

Probationary period reports - EDA

Opinion of 14 October 2013 on the notification for prior-checking regarding EDA's probationary period reports (Case 2013-0742)

Leave management - Artemis

Opinion of 14 October 2013 on the notification for prior checking from the Data Protection Officer of the Artemis Joint Undertaking on leave management (Case 2013-0346)

Attestation and Certification - F4E

Opinion of 14 October 2013 on the notifications for prior checking from the Data Protection Officer of the European Joint Undertaking for ITER and the Development of Fusion for Energy on Attestation and Certification (Case 2013-708)

Leave management - EMSA

Opinion of 8 October 2013 on the notification for prior checking from the Data Protection Officer of the European Maritime Safety Agency concerning leave management (Case 2013-0474)

Leave management - EIF

Opinion of 2 October 2013 on the notification of prior checking from the Data Protection Officer of the European Investment Fund (Case 2013-0349)

Requests to work part-time - Ombudsman

Opinion of 2 October 2013 on the notification for prior checking from the Data Protection Officer of the European Ombudsman on requests to work part-time (Case 2013-0507)

Leave requests

Opinion of 2 October 2013 on the notification for prior checking from the Data Protection Officer of the European Joint Undertaking for ITER and the Development of Fusion Energy concerning leave requests (Case 2013-0323)

Administrative inquiries and disciplinary proceedings - ENISA

Opinion of 1 October 2013 on the notification for prior checking notification of the processing of personal data in the framework of administrative inquiries and disciplinary proceedings at ENISA (Case 2013-0715)

Assessment of probationary staff - Ombudsman

Avis du 1 octobre 2013 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Médiateur européen à propos de l'évaluation du personnel stagiaire (Dossier 2013-0533)

Selection of the Chair of the Supervisory Board - ECB

Opinion of 20 September 2013 concerning a notification for prior checking pursuant to Article 27(4) of Regulation (EC) 45/2001 concerning the selection of the Chair of the Supervisory Board to the EDPS (Case 2013-1007)

Recruitment procedure for interim staff - EP

Opinion of 10 September 2013 on the notification for prior checking concerning the processing of personal data in the course of the EP's recruitment procedure for interim staff (Case 2013-0799)

Allegro HR management system - EU-OSHA

Opinion of 9 September 2013 regarding Allegro at the European Agency for Safety and Health at Work, including Flexitime (Cases 2011-1102 and 2013-0236)

Underperformance Procedure - ECB

Opinion of 30 August 2013 on the notification for prior checking received from the Data Protection Officer of the European Central Bank concerning the ECB's Underperformance Procedure (Case 2013-0892)

Leave management - EFCA

Opinion of 29 August 2103 on the notification for prior checking from the Data Protection Officer of the European Fisheries Control Agency concerning the management of leave, sickness related absences and other absences (Case 2013-0456)

Management of recuperation time - DG Interpretation

EDPS opinion of 18 July 2013 on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the management of recuperation time for staff interpret-

ers in DG Interpretation via the application 'INDISPONIBILITE'

Investigative Data Consultation Platform - OLAF

Opinion of 18 July 2013 on the notification for prior checking from the Data Protection Officer of the European Anti-Fraud Office (OLAF) regarding the Investigative Data Consultation Platform (Case 2012-0280)

Recruitment of confidential counsellors - ECHA

Opinion of 17 July 2013 on a notification for prior checking relating to the 'recruitment of confidential counsellors' at the European Chemicals Agency (ECHA) (Case 2013-0572)

Medical control examinations - F4E

Opinion of 16 July 2013 on a notification for prior checking concerning the processing operations relating to medical control examinations during an absence due to sickness or accident (the medical control procedure) at Fusion for Energy (F4E)(Case 2012-0864)

Invalidity procedure before the Invalidity Committee - F4E

Opinion of 16 July 2013 on a notification for Prior Checking received from the Data Protection Officer of F4E regarding the 'Invalidity procedure before the Invalidity Committee' (Case 2012-0863)

Joint Deployment Plans in EU waters - EFCA

Opinion of 16 July 2013 on a notification for Prior Checking received from the Data Protection Officer of the European Fisheries Control Agency regarding the 'processing of inspection reports related to Joint Deployment Plans in EU waters' (Case 2013-0539)

Video-surveillance system - EFSA

EDPS opinion of 16 July 2013 on the video-surveillance system at the European Food Safety Authority (EFSA) (Case 2013-0429)

Leave and absence management - ETF

Opinion of 4 July 2013 on the notification for prior checking from the Data Protection Officer of the European Training Foundation concerning leave and absence management (Case 2013-0234)

Leave management - FRA

Opinion of 4 July 2013 on a notification for prior checking received from the Data Protection Officer of the European Union Agency for Fundamental Rights regarding the processing of personal data on management of leave (Case 2013-0352)

Leave management - Cedefop

Opinion of 3 July 2013 on the notification for prior checking from the Data Protection Officer of the European Centre for the Development of Vocational Training concerning leave management (Case 2012-0265)

Leave and Absence Management - ERCEA

Opinion of 21 June 2013 on the notification for prior checking from the Data Protection Officer of the European Research Council concerning Leave and Absence Management (Case 2013-0327)

Leave and flexitime - EACEA

Opinion of 21 June 2013 on a notification for prior checking received from the Data Protection Officer of the Education, Audiovisual and Culture Executive Agency regarding processing of personal data in the area of leave and flexitime

Leave Management - EASA

Opinion of 20 June 2013 on the notification for prior checking from the Data Protection Officer of the European Aviation Safety Agency concerning Leave Management (Case 2011-1096)

Recording of switchboard and security room phone conversations - EIB

Opinion of 20 June 2013 on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank regarding the recording of switchboard and security room phone conversations (Case 2013-0297)

Leave management - EACI

Opinion of 20 June 2013 on the notification for prior checking from the Data Protection Officer of the Executive Agency for Competitiveness and Innovation on Leave management (Case 2013-0335)

Security Trustworthiness Check - JRC

Opinion of 19 June 2013 on a notification for Prior Checking received from the Data Protection Officer of the Commission on the Security Trustworthiness Check at the Joint Research Centre Ispra (Case 2012-1090)

Recruiting personnel - EC

Opinion of 19 June 2013 on a notification for prior checking notification on the selection procedures in view of recruiting personnel to the European agency eu-LISA from DG HOME (Case 2013-0156)

Management of absences and working hours - Committee of the Regions

Opinion of 18 June 2013 on the notification for prior checking from the Data Protection Officer of the Committee of the Regions concerning management of absences and time off and of working hours (Case 2013-0342)

PERSEO - European Ombudsman

Opinion of 12 June 2013 on the notification for prior checking from the Data Protection Officer of the European Ombudsman on PERSEO (Case 2013-0235)

Contract management system - EIB

Opinion of 7 June 2013 on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank regarding the PJ-CMS - PJ contract management system with integrated consultants' register (Case 2013-0034)

Work patterns, leave and presence management - REA

Opinion of 4 June 2013 on the notification for prior checking from the Data Protection Officer of the Research Executive Agency concerning work patterns, leave and presence management (Case 2012-0952)

Leave management - EEA

Opinion of 4 June 2013 on the notification for prior checking from the Data Protection Officer of the European Environment Agency concerning leave management (Case 2011-0851)

Managing potential conflicts of interest of Members of the Executive Committee - F4E

Opinion of 30 May 2013 on a notification for Prior Checking received from the Data Protection Officer of Fusion for Energy, The European Joint Undertaking for ITER and the Development of Fusion Energy, regarding the practical arrangements for managing potential conflicts of interest of Members of the Executive Committee of Fusion for Energy (Case 2013-0269)

Sick and Family leave management - FCH JU

Opinion of 27 May 2013 on the notification for prior checking from the Data Protection Officer of the Fuel Cells and Hydrogen Joint Undertaking concerning Sick and Family leave management (Case 2011-0836)

Annual appraisal - EEAS

Opinion of 23 May 2013 on the notification for prior checking from the Data Protection Officer of the European External Action Service concerning annual appraisal (Case 2013-0206)

Leave management - EU-OSHA

Opinion of 14 May 2013 on the notification for prior checking from the Data Protection Officer of the European Agency for Safety and Health at Work concerning leave management (Case 2013-0281)

Special leave - Eurofound

Opinion of 8 May 2013 on the notification for prior checking from the Data Protection Officer of the European Foundation for the Improvement of Living and Working Conditions concerning Special leave (Case 2013-0272)

Leave procedures - EASO

Opinion of 29 April 2013 on the notification for prior checking from the Data Protection Officer of the European Asylum Support Office concerning leave procedures (Case 2013-0248)

Processing operations concerning badge use - EFSA

Opinion of 9 April 2013 on a prior checking notification of the processing operations concerning badge use as an informative tool to staff on office presence in the context of time tracking (Case 2013-0171)

Harassment - ERA

Opinion of 9 April 2013 on a notification for prior-checking concerning the processing operations related to the informal procedure for cases of psychological and sexual harassment and the selection of confidential counsellors for the informal procedure in cases of harassment in the European Railway Agency (ERA) (Cases 2012-0902/3)

Unsolicited job applications - ERCEA

Opinion of 9 April 2013 on a notification for prior-checking concerning 'unsolicited job applications' at ERCEA (Case 2013-0181)

Procédure d'attestation - Médiateur Européen

Avis du 9 avril 2013 sur la notification d'un contrôle préalable du CEPD concernant la procédure d'attestation au Médiateur Européen (Dossier 2013-0217)

'Individual Production Monitoring' - Council

Opinion of 25 March 2013 on a notification for prior checking regarding the processing of personal data in the framework of the 'Individual Production Monitoring', Council of the European Union (Case 2013-0017)

Security Investigations - Joint Research Centre Petten

Opinion of 19 March 2013 on a notification for Prior Checking received from the Data Protection Officer of the Commission on the Security Investigations at the Joint Research Centre Petten (Case 2012-0782)

Self-perception questionnaire 'PERFORMANSE'

Opinion of 15 March 2013 on the notification for prior checking received from the Data Protection Officer of the European Commission regarding a self-perception questionnaire 'PERFORMANSE' organised by the European Administrative School (Case 2012-0590)

Analysis and transfer of information related to fraud to OLAF

Opinion of 14 March 2013 on a notification for Prior Checking received from the Data Protection Officer of EACI regarding the 'Analysis and transfer of information related to fraud to OLAF' (Case 2012-0652)

Selection and recruitment of Seconded National Experts - ERCEA

Opinion of 28 February 2013 on a notification for prior-checking regarding the processing of personal data in the context of the selection and recruitment of Seconded National Experts ('SNEs'), trainees and interim agents at the European Research Council Executive Agency (Case 2012-0997)

Administrative inquiries and disciplinary proceedings - ECDC

Opinion of 27 February 2013 on a notification for prior-checking on the processing of administrative inquiries and disciplinary proceedings at the European Centre for Disease Prevention and Control (Case 2012-1088)

Centre de développement externe - Conseil de l'Union européenne

Avis du 25 février 2013 sur la notification d'un contrôle préalable reçue du Délégué à la protection des données du Conseil de l'Union Européenne concernant la participation des agents du Secrétariat Général à un centre de développement externe (Dossier 2012-0773)

AML-CFT data processing - EIB

Opinion of 7 February 2013 on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank regarding AML-CFT data processing (Case 2012-0326)

Security investigations - EEAS

Opinion of 1 February 2013 on a notification for Prior Checking received from the Data Protection Officer of the European External Action Service on security investigations (Case 2011-1059)

Quality Management System - Ex-post Quality Checks - OHIM

Opinion of 29 January 2013 on the notification for prior checking received from the Data Protection Officer of the Office for Harmonization for the Internal Market ('OHIM') concerning OHIM's Quality Management System - *Ex-post* Quality Checks (Case 2012-0999)

Staff evaluation procedures - ECDC

Joint Opinion of 11 January 2013 on the notifications for prior checking from the Data Protection Officer of the European Centre for Disease Prevention and Control regarding staff evaluation procedures (Cases 2012-881, 2012-883 and 2012-884)

List of Non Prior Checks

SSM Chair and Vice-Chair Appointment - Council of the EU

Letter of 20 December 2013 regarding the notification for prior-checking concerning the Appointment of the Chair and the Vice-Chair of the Supervisory Board (Single Supervisory Mechanism) (Case 2013-1238)

Establishment of individual entitlements - EASA

Letter of 20 December 2013 on the prior check notification concerning the establishment of individual

entitlements of European Agency for Aviation Safety (EASA) staff members (Case 2013-1222)

EDPS Selection Procedure - Council of the EU

Reply of 20 December 2013 regarding processing operations concerning the Selection Procedure for the European Data Protection Supervisor and Assistant Supervisor (Case 2013-1243)

Management of Sysper 2 - TEN-T

Letter of 19 December 2013 on the prior checking notification concerning the 'management of Sysper 2' by the Trans-European Transport Network Executive Agency (TEN-T) (Case 2013-1287)

Procédure de sélection du CEPD - Commission

Lettre du 16 décembre 2013 concernant le mise à jour d'une notification concernant la sélection de candidats pour le poste de Contrôleur européen de la protection des données (CEPD) et le poste de Contrôleur adjoint (Dossier 2013-1334)

Local agents - EIB

Opinion of 5 November 2013 on a notification prior check notification regarding EIB local agents (Case 2013-0606)

Personal data processing operation relating to ENISA staff mobile phone bill payment

Letter of 31 October 2013 on the prior checking notification of a personal data processing operation relating to ENISA staff mobile phone bill payment (Case 2013-1156)

Ex-post audits - EACI

Letter of 9 October 2013 regarding the EACI notification for prior-checking on *ex-post* audits (Case 2013-0826)

Access control to premises - EDA

Letter of 1 October 2013 on the notification for prior-checking concerning access control to European Defence Agency (EDA) premises (Case 2013-0765)

Establishment of rights upon appointment or departure of staff - F4E

Letter of 10 September 2013 on the prior checking notification of the establishment of rights and entitlements upon departure of staff (Case 2013-0728) and the establishment of rights upon recruitment/ appointment of staff at Fusion for Energy (Case 2013-0729)

Complaints and Requests - F4E

Letter of 10 September 2013 concerning *ex-post* prior-checking notification regarding F4E's 'Complaints and Requests' (Case 2013-0709)

Security clearance management - EDA

Letter of 10 September 2013 on the prior checking notifications concerning the management of Facility Security Clearances (FSC) and Personnel Security Clearance (PSC) at the European Defence Agency (Cases 2013-0763 and 2013-0764)

Transfer of pension rights - F4E

Letter of 5 September 2013 concerning the prior checking notification relating to 'requests for transfer of pension rights' at Fusion for Energy (Case 2013-0706)

Management of personal files - EEA

Letter of 2 September 2013 on the prior checking notification of the management of personal files at the European Environment Agency (EEA) (Case 2013-0793)

Staff Expertise - ERCEA

Letter of 7 May 2013 on the prior checking notification of the processing operations concerning the ERCEA Department B-List on Staff Expertise (Case 2013-0166)

Use of badge - EFSA

Letter of 9 April 2013 on the prior checking notification of the processing operations concerning badge use as an informative tool to staff on office presence in the context of time tracking (Case 2013-0171)

Transfer of Data to the Scientific Council - ERCEA

Letter of 8 April 2013 regarding a notification for prior-checking on the 'Transfer of Data to the Scientific Council' by the ERCEA (Case 2013-0831)

Authorisation to engage in an outside activity - EASA

Letter of 23 February 2013 regarding the notification for prior checking of the processing operations concerning the 'EASA's Authorisation to engage in an outside activity or to carry out an assignment outside the Union' (Case 2012-1039)

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

Opinions on legislative proposals

Payment Services

Opinion of 5 December 2013 on a proposal for a Directive of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2006/48/EC and 2009/110/EC and repealing Directive 2007/64/EC, and for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions

European Single Market for Electronic Communications

Opinion of 14 November 2013 on the Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012

Electronic invoicing in public procurement

Opinion of 11 November 2013 on the Commission Proposal for a Directive of the European Parliament and the Council on electronic invoicing in public procurement

Deployment of the eCall System

Opinion of 29 October 2013 on the proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall system and amending Directive 2007/46/EC

Passenger Name Record data - Agreement between Canada and the European Union

Opinion of 30 September 2013 on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data

Entry/Exit System (EES) and Registered Traveller Programme (RTP)

Opinion of 18 July 2013 on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)

Community Trade Mark

Opinion of 11 July 2013 on the Proposal for a Directive of the European Parliament and of the Council to approximate the laws of the Member States relating to trade marks (recast) and the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 207/2009 on the Community trade mark

Prevention of money laundering and terrorist financing

Opinion of 4 July 2013 on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds

Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace

Opinion of 14 June 2013 on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union

European Union Agency for Law enforcement Cooperation and Training (Europol)

Opinion of 31 May 2013 on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA

Transparency of measures regulating the prices of medicinal products

Opinion of 30 May 2013 on the amended Commission proposal for a Directive on the transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of public health insurance systems.

Market Surveillance

Opinion of 30 May 2013 on the Commission Proposal for a Regulation of the European Parliament and the

Council on market surveillance of products and amending various legislative instruments of the European Parliament and of the Council

European Information Exchange Model (EIXM)

Opinion of 29 April 2013 on the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)

Drug Precursors

Opinion of 23 April 2013 on proposals for a Council decision on the signature and for a Council decision on the conclusion of the Agreement between the European Union and the Russian Federation on drug precursors

Civil Aviation

Opinion of 10 April 2013 on the Commission Proposal for a Regulation on occurrence reporting in civil aviation and repealing Directive No 2003/42/EC, Commission Regulation (EC) No 1321/2007, Commission Regulation (EC) No 1330/2007 and Article 19 of Regulation (EU) No 996/2010

The Digital Agenda for Europe

Opinion of 10 April 2013 on the Communication from the Commission on 'The Digital Agenda for Europe - Driving European growth digitally'

Insolvency Proceedings

Opinion of 27 March 2013 on the European Data Protection Supervisor on the Commission proposal for a Regulation amending Council Regulation (EC) No 1346/2000 on insolvency proceedings

eHealth Action Plan 2012-2020

Opinion of 26 March 2013 on the Communication from the Commission on 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century'

In Vitro Diagnostic Medical Devices

Opinion of 8 February 2013 on the Commission proposals for a Regulation on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and a Regulation on in vitro diagnostic medical devices

Drug precursors

Opinion of 18 January 2013 on the Proposal for a Regulation amending Regulation (EC) No 273/2004 on drug precursors and the Proposal for a Regulation amending Council Regulation (EC) No 111/2005 laying down rules for the monitoring of trade between the Community and third countries in drug precursors

Formal comments on legislative proposals

General Data Protection Regulation

EDPS comments of 9 December 2013 on the application of the proposed General Data Protection Regulation

Guidelines for the reuse of public sector information (PSI)

EDPS comments of 22 November 2013 in response to the public consultation on the planned guidelines on recommended standard licences, datasets and charging for the reuse of public sector information initiation by the European Commission.

Supervision on Europol

Letter of 13 November 2013 to LIBE Committee of the European Parliament concerning the data protection supervision on Europol

Administrative cooperation in the field of taxation

EDPS Comments of 5 November 2013 on the proposal for a Council Directive amending Directive 2011/16/EU on administrative cooperation in the field of taxation

Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values

EDPS Comments of 30 August 2013 on the Commission Green Paper: 'Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values'.

Sale of Counterfeit Goods via the Internet

EDPS Comments of 11 July 2013 on the Report from the Commission to the European Parliament and the Council on the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet

Payment accounts

EDPS Comments of 27 June 2013 on the Consultation on proposal for a Directive of the European Parliament and of the Council on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features

Intelligent transport systems

EDPS Comments of 13 June 2013 on the Commission Delegated Regulations supplementing Directive 2010/40/EU of the European Parliament and the Coun-

cil with regard to "Data and procedures for the provision, where possible, of road safety related minimum universal traffic information free of charge to users' and "Provision of information services for safe and secure parking places for trucks and commercial vehicles'

European company law and corporate governance

EDPS Comments of 27 March on the Action Plan: European company law and corporate governance - a modern legal framework for more engaged shareholders and sustainable companies

Data Protection Reform Package

EDPS additional Comments of 15 March 2013 on the Data Protection Reform Package

Harmonisation of the laws of the Member States

EDPS Comments of 27 February 2013 on the Proposal for a Directive 'on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment', replacing the R&TTE Directive 1995/5/EC

Annex G — Speeches by the Supervisor and Assistant Supervisor in 2013

The Supervisor and the Assistant Supervisor continued to invest substantial time and effort in 2013 to explain their mission and to raise awareness of data protection in general. They also addressed a number of specific issues in speeches delivered at various events that were held in the EU institutions, member states and beyond.

European Parliament

10 January	Assistant Supervisor, LIBE Committee on Data Protection Reform (Brussels) (*)
28 January	Supervisor and Assistant Supervisor, Conference on the Data Protection Day (Brussels)
19 February	Supervisor, STOA conference on e-Government (Brussels) (*)
19 March	Supervisor, LIBE Rapporteurs on Data Protection Reform (Brussels)
20 March	Supervisor, LIBE Committee on Data Protection Reform (Brussels)
29 May	Supervisor and Assistant Supervisor, LIBE Committee on Annual Report 2012 (Brussels)
19 June	Supervisor, Privacy Platform on Definition of Personal Data (Brussels)
20 June	Supervisor, Inter-Parliamentary Committee on Stockholm Programme (Brussels) (*)
7 October	Supervisor, LIBE Committee Inquiry on Electronic mass surveillance (Strasbourg) (*)
28 November	Supervisor, IMCO Committee on e-Call Regulation (Brussels)
5 December	Supervisor, Greens' conference on Anti-Money Laundering (Brussels)

Council

22 January	Supervisor, Polish Permanent Representation on Data Protection Day (Brussels)
25 April	Assistant Supervisor, Council WP on Insolvency Proceedings (Brussels)
5 September	Supervisor, Council WP on proposed Europol Regulation (Brussels)
17 September	Supervisor, Presidency conference on European Public Prosecutor (Vilnius)

European Commission

19 March	Assistant Supervisor, Group of Resource Directors Meeting (Brussels)
14 June	Supervisor, European Administrative School lunchtime conference (Brussels)
15 October	Supervisor, European Group on Ethics on Data Protection Reform (Brussels)
18 October	Supervisor, EU Anti-Trafficking Coordinator conference (Vilnius)
14 November	Supervisor, European Administrative School lunchtime conference (Brussels)

Other EU institutions and bodies

22 January	Supervisor and Assistant Supervisor, EDPS Strategic Review (Brussels)
28 January	Supervisor, Data Protection Day - Art Exhibition (Brussels) (*)
17 April	Assistant Supervisor, Training for EU Data Protection Officers (Brussels)
6 March	Supervisor, EESC Conference on responsible use of Internet (Brussels) (*)
12 June	Assistant Supervisor, EDPS Workshop on Electronic Communications (Brussels)
24/26 June	Supervisor and Assistant Supervisor, EIPA Data Protection Certification and training programme (Maastricht)
4 July	Supervisor, EUI Summer Academy on European Data Protection Law (Florence)
19 September	Assistant Supervisor, EDPS Workshp on Website and Mobile Devices (Brussels)
11 October	Supervisor, Frontex Conference on Automated Border Control (Warsaw)

18 November	Supervisor, ERA Conference on European Data Protection Law (Trier) (*)
2 December	Supervisor, Expert Forum on Internet and Data Protection at ECJ (Luxembourg)
11 December	Supervisor, ENISA Conference on Cyber Security (Brussels)

International Conferences

9 January	Supervisor, Conference on Ethical Dimensions of Privacy (Tallinn) (*)
25 January	Supervisor, Conference on Computers, Privacy and Data Protection (Brussels)
31 January	Assistant Supervisor, International Taiex Workshop on Data Protection (Zagreb)
21 March	Supervisor, CONSENT Conference on Data Protection Review (Malta)
24 April	Supervisor, IAPP Intensive on Data Protection Review (London)
14 May	Supervisor, European Data Protection Day (Berlin)
16 May	Supervisor and Assistant Supervisor, European Data Protection Conference (Lisbon)
30 May	Supervisor, UN Conference on e-Government (Helsinki)
26 September	Supervisor, International Data Protection Conference (Warsaw) (*)
10 October	Supervisor, IIC Telecommunication and Media Forum (London)
24 October	Assistant Supervisor, Data Protection in the Judiciary (Budapest) (*)
6 December	Supervisor, Council of Europe Conference on Cybercrime (Strasbourg)
11 December	Supervisor, IAPP panel on Trans-Border Data Flows (Brussels)

Other events

23 January	Supervisor, Hearing on Data Protection Review in Dutch Parliament (The Hague)
23 January	Supervisor, Future of Privacy Forum on Data Protection Review (Brussels)
23 January	Assistant Supervisor, Computer, Privacy & Data Protection Conference (Brussels)
8 February	Supervisor, SURF Conference on Data Protection Review (Amsterdam)
19 February	Supervisor, CIPL Workshop on Analytics (Brussels)
21 February	Supervisor, Accountability workshop (Warsaw)
22 February	Assistant Supervisor, Italian Senate on the EU Reform and Health Data (Rome)
5 March	Assistant Supervisor, Future of Privacy Forum on Privacy by Design (Washington DC)
5 March	Assistant Supervisor, Briefing to EU MS Representatives on the EU Reform (Washington DC)
8 March	Assistant Supervisor, IAPP Global Privacy Summit (Washington DC)
14 March	Supervisor, Dutch Ministry of Justice on Data Protection Review (The Hague)
15 March	Supervisor, French Bar Association on European Data Protection Law (Brussels) (*)
26 March	Supervisor, Westminster e-Forum on Data Protection Review (London)
27 March	Supervisor, C-PET Briefing on Data Protection Review (Brussels)
28 March	Supervisor, Le Point Conference on Connected and Intelligent Home (Paris) (*)
4/5 April	Supervisor and Assistant Supervisor, Data Protection in Criminal Proceedings (Barcelona)
8 April	Assistant Supervisor, CEPS Digital Forum on Online Data Processing (Brussels)
13 April	Assistant Supervisor, Privacy and Openness, Italian Administrative Judiciary (Rome)
16 April	Supervisor, Forum on EU-US Legal and Economic Affairs (Brussels)
19 April	Assistant Supervisor, Italian Superior School for Economy and Finance (Rome)

23 April	Supervisor, EMC Seminar on Big Data (Breukelen)
23 April	Supervisor, Hogan Lovells on Data Protection Review (London)
24 April	Assistant Supervisor, French Bar Association (Paris) (*)
13 May	Supervisor, HUB Lecture on Data Protection Review (Brussels)
20 May	Supervisor, Privacy Law Forum (Chantilly)
21 May	Assistant Supervisor, Lithuanian Ministry of Justice on Data Protection Review (Vilnius)
23 May	Assistant Supervisor, Privacy Day Forum (Pisa)
30 May	Assistant Supervisor, Customer in Control in an Age of Ubiquitous Data (Brussels)
5 June	Supervisor, Health Privacy Summit (Washington DC)
13 June	Supervisor, Seminar Covington on DP and Competition (Brussels) (*)
20 June	Supervisor, Wilson & Sonsini Book presentation (Brussels)
2 July	Supervisor, EFC Workshop on Data Protection and Research (Brussels)
5 July	Assistant Supervisor, Conference on the EU Data Protection Review (Barcelona)
9 July	Assistant Supervisor, University, Institute for Information Law (Amsterdam)
10 July	Supervisor, EPC on Post Stockholm Programme (Brussels)3 September Supervisor, CEPS Policy meeting on Smart Borders (Brussels)
4 September	Supervisor, EPIF Worksop on Anti-Money Laundering (Brussels)
10 September	Supervisor, 12th Annual Data Protection Conference (London)
12 September	Supervisor, Forum on EU-US Legal and Economic Affairs (Berlin)
17 September	Assistant Supervisor, 4th Annual European DP and Privacy Conference (Brussels)
18 September	Supervisor, DMEXCO on Privacy on the Internet (Cologne)
19 September	Supervisor, Digital Enlightenment Forum (Brussels) (*)
20 September	Supervisor, European Banking Federation (Brussels)
24 September	Assistant Supervisor, Phaedra Project First Workshop (Warsaw)
30 September	Supervisor, Freedom not Fear (Brussels)
30 September	Supervisor, Rotary on Data Protection after Snowden (Tervuren)
2 October	Assistant Supervisor, Benzi Foundation on Biotech and Innovative Science (Bari)
4 October	Assistant Supervisor, Confederation of Industry on the EU Reform (Rome)
14 October	Supervisor, Compliance Week on Data Protection Review (Brussels)
22 October	Supervisor, European Voice Data Protection Conference (Paris)
25 October	Supervisor, Data Protection in Criminal Proceedings (Barcelona)
30 October	Supervisor, Europa Institute Lecture on Data Protection Reform (Zurich) (*)
31 October	Supervisor, University of Zurich Conference on Big Data (Zurich)
7 November	Supervisor, BBA Seminar on Data Protection Review (London)
12 November	Supervisor, Data Protection Conference (Valencia-Castellon)
25 November	Supervisor, King's College Alumni Association (Brussels)
30 November	Supervisor, CCBE Plenary on Mass Surveillance (Brussels)
3 December	Supervisor and Assistant Supervisor, AECA on DP Review (Brussels)
12 December	Assistant Supervisor, IAPP Europe Data Protection Congress 2013 (Brussels)

(*) Text available on the EDPS website

Annex H — Composition of EDPS Secretariat

The EDPS and Assistant EDPS with most of their staff.

Director, Head of Secretariat

Christopher DOCKSEY

• Supervision and Enforcement

Sophie LOUVEAUX *Acting Head of Unit*	Maria Verónica PEREZ ASINARI *Head of Administrative Consultations*
Delphine HAROU *Head of Prior Checks*	Stephen ANDREWS *Supervision and Enforcement Assistant*
Raffaele DI GIOVANNI BEZZI* *Legal Officer*	Daniela GUADAGNO *Legal Officer/Seconded National Expert*
Ute KALLENBERGER *Legal Officer*	Xanthi KAPSOSIDERI *Legal Officer*
Owe LANGFELDT *Legal Officer*	Antje PRISKER *Legal Officer*
Bénédicte RAEVENS *Legal Officer*	Dario ROSSI *Supervision and Enforcement Assistant Accounting Correspondent Financial ex-post facto verifier*
Tereza STRUNCOVA *Legal Officer*	Michaël VANFLETEREN *Legal Officer*

• Policy and Consultation

Hielke HIJMANS *Head of Unit*	Anna BUCHTA *Head of litigation and legislative policy*
Herke KRANENBORG* *Head of litigation and legislative policy*	Anne-Christine LACOSTE *Head of international cooperation and legislative* policy
Zsuzsanna BELENYESSY *Legal Officer*	Gabriel Cristian BLAJ *Legal Officer*
Alba BOSCH MOLINE *Legal Officer*	Isabelle CHATELIER *Legal Officer*
Christian D'CUNHA *Legal Officer*	Priscilla DE LOCHT *Legal Officer*
Elena JENARO *Legal Officer*	Amanda JOYCE *Policy and Consultation Assistant*
Elise LATIFY *Legal Officer*	Per JOHANSSON *Legal Officer*
Vera POZZATO *Legal Officer*	Galina SAMARAS* *Policy and Consultation Assistant*

• IT Policy

Achim KLABUNDE *Head of sector*	Massimo ATTORESI *Technology and Security Officer*
Andy GOLDSTEIN *Technology and Security Officer LISO*	Luisa PALLA *Records Managers/Archivist*
Bart DE SCHUITENEER *Technology Officer*	Hannes TSCHOFENIG* *Technology Officer*

• Records management Group

Andrea BEACH* *Head of Sector*	Marta CORDOBA-HERNANDEZ *Administrative Assistant*
Kim DAUPHIN* *Administrative Assistant/Interim*	Alicia DUARTE *Administrative Assistant*
Milena KEMILEVA *Administrative Assistant*	Milan KUTRA* *Administrative Assistant*
Kim Thien LÊ *Administrative Assistant*	Séverine NUYTEN *Administrative Assistant*
Ewa THOMSON* *Administrative Assistant*	

(*) Staff members who left the EDPS in the course of 2013

• Information and Communication

Olivier ROSSIGNOL *Head of Sector*	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*	Maria SANCHEZ LOPEZ *Head of Finance*
Pascale BEECKMANS *Finance Assistant* *GEMI*	Laetitia BOUAZZA-ALVAREZ *Administration Assistant*
Fabienne DUCAUD *Administration Assistant*	Anne LEVÊCQUE *Human Resources Assistant* *& official managing leave*
Vittorio MASTROJENI *Human Resources Officer*	Julia MOLERO *Finance Assistant*
Daniela OTTAVI *Finance and Procurement Officer*	Aida PASCU *Administration Assistant* *LSO*
Sylvie PICARD *Data Protection Officer* *Internal Control Coordinator*	Anne-Françoise REYNDERS *Human Resources Assistant* *& Training coordinator*

The European Data Protection Supervisor

Annual Report 2013

Luxembourg: Publications Office of the European Union, 2014

2013 — 125 pp. — 21 × 29.7 cm

ISBN 978-92-95076-87-7
doi: 10.2804/59280

EUROPEAN DATA
PROTECTION SUPERVISOR

QT-AA-14-001-EN-C

The European guardian of data protection

www.edps.europa.eu

Publications Office

@EU_EDPS