ISSN 1830-5474

Annual Report

2012

European Data Protection Supervisor

Annual Report

2012

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

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

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

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2013

ISBN 978-92-95076-78-5
doi:10.2804/52280

© European Union, 2013
Reproduction is authorised provided the source is acknowledged.
© Photos: iStockphoto/EDPS, European Parliament, European Ombudsman, European Conference of Data Protection Commissions, WCO.

Printed in Belgium

Printed on elemental chlorine-free bleached paper (ECF)

Contents

User guide 7
Mission statement, values and principles 9
Foreword 11

1 2012 HIGHLIGHTS

1. 2012 HIGHLIGHTS 12

1.1. General overview of 2012 12
1.2. Vision and methodology: the Strategic Review, Rules of Procedure and Annual Management Plan 17

2 SUPERVISION AND ENFORCEMENT

2. SUPERVISION AND ENFORCEMENT 20

2.1. Introduction 20
2.2. Data Protection Officers 21
2.3. Prior checks 22
2.3.1. Legal base 22
2.3.2. Procedure 22
2.3.3. Main issues in prior checks 25
2.3.4. Consultations on the need for prior checking 28
2.3.5. Notifications not subject to prior checking or withdrawn 29
2.3.6. Follow-up of prior checking opinions 30
2.3.7. Conclusions 31
2.4. Complaints 31
2.4.1. The EDPS mandate 31
2.4.2. Procedure for handling of complaints 31
2.4.3. Confidentiality guaranteed to the complainants 34
2.4.4. Complaints dealt with in 2012 34
2.5. Monitoring compliance 36
2.5.1. General monitoring and reporting: 2011 Survey 37
2.5.2. Visits 37
2.5.3. Inspections 38
2.6. Consultations on administrative measures 40
2.6.1. Consultations under Articles 28.1 and 46(d) 40
2.7. Data protection guidance 44
2.7.1. Thematic Guidelines 44
2.7.2. Training and workshops 45
2.7.3. DPO Corner and other tools 45

3 CONSULTATION

3. CONSULTATION 46

3.1. Introduction: overview of the year and main trends 46
3.2. Policy framework and priorities 47
3.2.1. Implementation of consultation policy 47
3.2.2. Results of 2012 48
3.3. Review of the EU Data Protection Framework 48
3.4. Area of Freedom, Security and Justice and international cooperation 50
3.4.1. EUROSUR 50
3.4.2. Freezing and confiscation of proceeds of crime in the European Union 50
3.4.3. European Cybercrime Centre 51
3.4.4. SIS II Migration 51
3.4.5. Human trafficking 51
3.4.6. EURODAC Regulation 52
3.4.7. CRIM Committee of the European Parliament 52
3.5. Internal Market including financial data 53
3.5.1. Administrative Cooperation in the field of Excise Duties 53
3.5.2. Review of the professional qualifications directive 53
3.5.3. Reform proposals for financial markets 53
3.5.4. Statutory audits 54
3.5.5. European venture capital funds & social entrepreneurship funds 54
3.5.6. Improving securities settlement in the European Union 54
3.5.7. Posting of workers in the framework of the provision of services 54
3.5.8. Insurance mediation, UCITS and key information documents for investment products 55

3.6. Digital Agenda and technology **55**
3.6.1. Cloud Computing 55
3.6.2. Open Data Package 56
3.6.3. Smart meters 56
3.6.4. Electronic Trust Services Regulation 57
3.6.5. Better Internet for Children 57
3.6.6. Network and Information Security in the EU 58
3.6.7. Open Internet and Net Neutrality 58
3.7. Public health and consumer affairs **58**
3.7.1. Cross-border Alternative Dispute Resolution for consumer disputes and a Regulation creating an Online Dispute Resolution platform 58
3.7.2. Early Warning Response System and cross-border threats to health 58
3.7.3. European Consumer Agenda 58
3.7.4. Clinical Trials 58
3.8. Publication of personal information **59**
3.9. Other issues **60**
3.10. EDPS policy on access to documents **60**
3.11. Court matters **61**
3.12. Priorities in 2013 **62**

4. COOPERATION 64

4.1. Article 29 Working Party **64**
4.2. Coordinated supervision **65**
4.2.1. EURODAC 65
4.2.2. VIS 65
4.2.3. CIS 66
4.3. European conference **66**
4.4. International conference **67**
4.5. Third countries and international organisations **67**
4.5.1. Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data 67
4.5.2. International Workshop on data protection in international organisations 68

5. MONITORING OF TECHNOLOGY 69

5.1. Technological development and data protection **69**
5.2. Future technological developments **70**
5.2.1. Data protection principles must work with new technologies 70
5.2.2. Business developments 70
5.2.3. Law enforcement and security 73
5.2.4. Other developments 75

6. INFORMATION AND COMMUNICATION 77

6.1. Introduction **77**
6.2. Communication 'features' **78**
6.2.1. Key audiences and target groups 78
6.2.2. Language policy 78
6.3. Media relations **78**
6.3.1. Press releases 79
6.3.2. Press interviews 79
6.3.3. Press conferences 79
6.3.4. Media enquiries 79
6.4. Requests for information and advice **79**
6.5. Study visits **80**
6.6. Online information tools **80**
6.6.1. Website 80
6.6.2. Newsletter 81
6.6.3. Twitter 81

6.7. Publications **82**
6.7.1. Annual Report 82
6.7.2. Thematic publications 82
6.8. Awareness-raising events **82**
6.8.1. Data Protection Day 2012 82
6.8.2. EU Open Day 2012 83

7 ADMINISTRATION, BUDGET AND STAFF

7. ADMINISTRATION, BUDGET AND STAFF 84

7.1. Introduction **84**
7.2. Budget, finance and procurement **84**
7.2.1. Budget 84
7.2.2. Finance 85
7.2.3. Procurement 86
7.3. Human resources **86**
7.3.1. Recruitment 86
7.3.2. Professionalising the HR function 86
7.3.3. Traineeship programme 88
7.3.4. Programme for seconded national experts 88
7.3.5. Organisation chart 88
7.3.6. Working conditions 88
7.3.7. Training 89
7.3.8. Social activities 90
7.4. Control functions **90**
7.4.1. Internal control 90
7.4.2. Internal audit 91
7.4.3. External audit 91
7.5. Infrastructure **92**
7.6. Administrative environment **92**
7.6.1. Administrative assistance and inter-institutional cooperation 92
7.6.2. Document management 92

8 EDPS DATA PROTECTION OFFICER

8. EDPS DATA PROTECTION OFFICER 94

8.1. The DPO at the EDPS **94**
8.2. The Register of processing operations **94**
8.3. EDPS 2012 Survey on the status of DPOs **95**
8.4. Information and raising awareness **95**

9 MAIN OBJECTIVES FOR 2013

9. MAIN OBJECTIVES FOR 2013 97

9.1. Supervision and enforcement **97**
9.2. Policy and consultation **98**
9.3. Cooperation **99**
9.4. Other fields **99**

Annex A — Legal framework 101
Annex B — Extract from Regulation (EC) No 45/2001 103
Annex C — List of abbreviations 105
Annex D — List of Data Protection Officers 107
Annex E — List of prior check opinions 110
Annex F — List of opinions and formal comments on legislative proposals 116
Annex G — Speeches by the Supervisor and Assistant Supervisor in 2012 120
Annex H — Composition of EDPS Secretariat 123

USER GUIDE

Following this guide, there is a mission statement and foreword to the 2012 Annual Report by Peter Hustinx, European Data Protection Supervisor and Giovanni Buttarelli, Assistant Supervisor.

Chapter 1 — **2012 Highlights** presents the main features of our work in 2012, the results of the Strategic Review and the results achieved 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 2012. It also includes information on the Guidelines adopted by the EDPS on consultations in the field of supervision and enforcement and Guidelines on the processing of personal information in the area of leave and flexitime

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. The chapter also outlines the involvement of the EDPS in cases before the Court of Justice of the EU. It contains an analysis of horizontal themes: new developments in policy and legislation and the ongoing review of the EU data protection legal framework.

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

Chapter 5 — **Monitoring of 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 key areas within the EDPS organisation including budget issues, human resource matters and administrative agreements.

Chapter 8 — **EDPS Data Protection Officer (DPO)** includes a report on the update of the EDPS' register of processing operations in 2012, resulting in 25 new notifications.

Chapter 9 — **Main objectives for 2013** gives an overview of our work and main priorities for 2013.

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 2012 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 2012 as the ninth 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 fourth year of our shared mandate as members of this authority.

Special efforts were made this year in improving the efficiency and effectiveness of our organisation during the present climate of austerity. In this context, we completed a thorough Strategic Review, resulting in clear objectives for 2013-2014, the adoption of internal Rules of Procedure covering all EDPS activities and the adoption of an Annual Management Plan.

In the course of 2012, we once again set new benchmarks in different areas of activity. 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 saw the effects of our new enforcement policy: most EU institutions and bodies, including many agencies, are making good progress in complying with the Data Protection Regulation, although there are still some which should increase their efforts.

In the consultation of new legislative measures, we issued a record number of opinions on a wide range of subjects. The Review of the EU legal framework for data protection was at the top of our agenda. However, the implementation of the Stockholm programme in the area of freedom, security and justice and the Digital Agenda, as well as 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.

We wish to take this opportunity to thank those in the European Parliament, the Council and the Commission who support 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 contributes greatly to our effectiveness.

Peter Hustinx
European Data Protection Supervisor

Giovanni Buttarelli
Assistant Supervisor

1 2012 HIGHLIGHTS

1.1. General overview of 2012

The main activities of the EDPS in 2012 continued to grow both in scale and scope at the same time as resources were effectively reduced in the light of budget constraints. The Strategic Review announced in the last Annual Report was completed and the resulting Strategy for 2013-2014 articulates the vision and the methodology required to improve our capacity to work effectively and efficiently in a climate of austerity. The Strategy was complemented by the adoption of Rules of Procedure and an Annual Management Plan. These documents are closely integrated and are discussed in Chapter 1.2 below.

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 supervisory bodies in the former 'third pillar' of the EU, involving police and judicial cooperation in criminal matters, 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 2012. However, some of the key elements are summarised in this section.

In 2012, a new sector for IT Policy was created to better deal with various issues relating to the use of new information technologies. This explains a greater emphasis on the monitoring of technology in Chapter 5.

The importance of information and communication in our core activities also continues to grow and our communication work in 2012 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.

Supervision and enforcement

The supervisory tasks of the EDPS are very broad and range from advising and supporting the work of data protection officers (DPOs), to providing

[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/agencies/community_agencies/index.en.htm

guidance and training, prior checking of risky processing operations or conducting inquiries, including on the spot inspections.

We consider DPOs to be key players in ensuring compliance with the data protection regulation. We have, therefore, continued to support the work of DPOs by attending DPO meetings, organising trainings or workshops for DPOs, meeting DPOs bilaterally when they have been in need of specific guidance, organising a helpline for DPO queries and developing a dedicated area for DPOs on our website.

In May 2012, as part of our efforts to support the work of DPOs, we launched a survey on the status of DPOs. Based on a questionnaire, the survey focused on the mandate, position and resources of the DPO so as to collect consistent information about the state and evolution of the DPO function. The conclusions of this exercise were compiled into a report which highlights a number of positive outcomes, but also some areas of concern which we intend to monitor closely.

Prior checking of risky processing operations continued to be an important aspect of supervision work. In 2012, we received 119 notifications for prior checking and adopted 71 prior checking opinions. After careful analysis, 11 cases were not subject to prior checking. In contrast to previous years where large EU institutions had been frequent addressees, in 2012, we addressed the majority of our opinions to EU agencies and bodies. In general, the opinions adopted in 2012 covered standard administrative procedures such as staff evaluation and processing of health data, but also core business activities such as processing operations related to asset freezing activities at the Commission, revised OLAF investigation procedures and annual declarations of interest. In the follow up of EDPS opinions, we were pleased to be able to close 92 cases in 2012.

In 2012, we received 86 complaints, a decrease of approximately 20% compared to 2011, thus confirming the effectiveness of the online complaint form in reducing the number of inadmissible complaints. Of these, 46 were inadmissible *prima facie*. The remaining 40 complaints led to more in-depth inquiries. Of those cases resolved in 2012, we found that there had been no breach of the data protection rules or that the necessary measures had been taken in 26 cases. Conversely in four cases, we found non-compliance with data protection rules and recommendations were addressed to the controller.

In addition to our general monitoring exercises, such as the one on the status of DPOs, we targeted our monitoring actions to areas where we had reason to be concerned about the level of compliance with the Regulation. In 2012, we **visited** six agencies where there was a suspected lack of engagement in compliance or a lack of communication between the agency and the EDPS. These visits proved to be very effective in raising awareness and committing management to respect the Regulation. We **inspected** 15 EU institutions or bodies and followed-up previous inspections.

On 23 November 2012, we issued a **policy on consultations in the field of supervision and enforcement**. This paper provides guidance to EU institutions and bodies and DPOs on consultations to the EDPS based on Articles 28(1) and 46(d) of the Regulation and stresses their accountability as institutions and the key role of their DPOs.

We have also provided guidance to EU institutions and agencies by adopting **Guidelines concerning the processing of personal information in the area of leave and flexitime**.

Consultation

Following the trend of previous years, 2012 saw our consultation work on legislation increase, with an all-time high of 33 opinions, 15 formal comments and 37 informal comments issued. The fact that increasing numbers of legislative proposals are submitted to us for consultation is reflected in our inventory and is testimony to the growing relevance and consideration of data protection in EU legislation.

We continued to be closely involved in the ongoing work on the reform of the EU data protection framework[4]. In response to the **proposal on the reform package** comprised of a regulation and a directive, published in January, we issued an opinion in March. Thereafter, we continued to highlight potential areas of concern and possible improvements in speeches, press releases and other forums throughout the year. Overall, we welcome the proposed regulation, an instrument **directly applicable** to the Member States, as a great step forward, but regret that a separate legal instrument, the proposed Directive, has been chosen to regulate the law enforcement area with a much lower level of protection. Since it **does not meet the requirement of a consistent and high level** of data protection, it is significantly inferior to the proposed regulation. The overriding weakness of the reform package is that it does not remedy the general lack of comprehensiveness in EU data protection rules.

The importance of data protection continues to grow: apart from the usual priorities of the Area of Freedom, Security and Justice (AFSJ) and international data transfers, opinions on the internal market and the health sector became increasingly common in 2012. At the same time, the rapid developments in the area of the Digital Agenda were mirrored by an influx of related legislative proposals. The following highlights include a selection of the opinions we adopted in these fields.

In the area of **AFSJ**, the question of necessity was a recurrent theme, as we saw law enforcement agencies arguing for increased access to other databases for crime prevention purposes. We cautioned against this trend of function creep and highlighted the potential harm it might cause as can be seen in our opinions on EURODAC, SIS II and the European Cybercrime Centre. Related issues in the area were excessive data transfers and an apparent disregard for the utility of implementing appropriate data protection principles in ensuring the success of law enforcement initiatives. We highlighted these concerns in our comments on EUROSUR and on the EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016, respectively.

In the **digital agenda and technology** domain, we published an opinion on cloud computing which highlighted the particular data protection challenges created by cloud computing in general and how these will be addressed under the proposed data protection regulation. The impact of new technology is – and will continue to remain – of the utmost importance in this area and pinpoints the need for the implementation of data protection principles such as *privacy by design* and *privacy by default*. This was also highlighted in our other opinions in this area, for example, smart meters, network and information security in the EU and on the open internet and net neutrality.

On the issue of the **internal market**, we issued a package of opinions on reform proposals for increased supervision of financial markets, mainly concerning the data protection impact of monitoring financial data and cross-border transfers. While the desire for more control of financial data might be justified, we emphasise that this type of data may also include personal information and related proposals are thus required to implement adequate safeguards. Other notable opinions of the year were issued on administrative cooperation in the field of excise duties, on statutory audits, on European venture capital funds & social entrepreneurship funds and on insurance mediation, UCITS and key information documents for investment products. A common recommendation from us was a clearer justification for the scope of investigatory powers of regulatory authorities.

Achieving a balance between transparency and data protection is a recurring theme in our work. In 2012, we adopted several opinions in different fields which dealt with the **publication of personal information**. These instances can themselves be divided into different categories such as: the re-use of public sector information (PSI) and the publication of personal information in the context of 'naming and shaming'. In these and other opinions we emphasised the need to balance the principle of transparency, the right to privacy and data protection and the need for specific safeguards.

[4] http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package

In **public health and consumer affairs**, we observed a growing trend to fuse new digital technologies with existing practices to improve the quality of service. These efforts are commendable and personalised care and services have great potential. However, given the sensitivity of personal health data, consumer trust in new services can only be fostered and maintained when fundamental data protection principles are respected. The consolidation of previously irrelevant data and information collected for other purposes remain a challenge specific to this field.

We also commented on other proposals, such as the establishment of the European voluntary humanitarian aid corps, a proposal on the deposit of the historical archives of the institutions at the European university Institute in Florence and on the proposal for a regulation on the statute and funding of European political parties and European political foundations.

Court cases

In 2012, we intervened in four cases before the Court of Justice of the EU and the Civil Service Tribunal.

The first case dealt with the alleged lack of independence of the Austrian data protection authority (DSK). The EDPS supported the position of the Commission which argued that the functional independence of the DSK provided for by Austrian law was not sufficient. The Court followed this reasoning and concluded that its close ties with the Austrian Federal Chancellery prevented the DSK from being above all suspicion of partiality.

The second case in which we intervened on the side of the applicant was *Egan and Hackett v. European Parliament* (Case T-190/10). This was the last of three cases in which the General Court had to rule on the relationship between the public access to documents regulation and the data protection regulation after the leading ruling in *Bavarian Lager v. Commission* of 29 June 2010 (Case C-28/08 P). As in the other two cases, the EDPS argued in favour of greater transparency

We intervened in two other cases which are still pending at the time of writing. The first case concerned an infringement proceeding against Hungary on the independence of the data protection authority. The second case, before the Civil Service Tribunal, concerned an alleged breach of the EU data protection Regulation (EC) No 45/2001 during an internal harassment investigation by the EIB.

We also closely followed several other cases without intervening such as the Spanish Google case which centres on the applicability of Spanish law implementing the European data protection directive with regard to Google activities and two other cases related to the validity of the European data retention directive.

Cooperation

The main platform for cooperation between data protection authorities in Europe is the **Article 29 Data Protection Working Party** (WP29), which plays an important role in the uniform application of the Data Protection Directive.

The EDPS and the WP29 have collaborated on a wide range of subjects, particularly for the opinions on purpose limitation and compatible use, smart grid data protection impact assessment templates and open data, where the EDPS acted as the rapporteur. We also made significant contributions to the opinions adopted on the data protection reform discussions, cloud computing, cookie consent exemption and developments in biometric technologies.

We have also been very active in the area of coordinated supervision of large-scale databases such as **EURODAC**, a European fingerprint database for identifying asylum seekers and irregular border-crossers. The EURODAC Supervision Coordination Group – composed of national data protection authorities and the EDPS – met twice in Brussels in 2012. The Group adopted a standardised inspection plan for EURODAC national access points (NAPs) to assist in national inspections and envisioned that a unified practice on dealing with unreadable fingerprints should be agreed upon once the corresponding report is finalised in 2013.

A similar arrangement governs the supervision of the **Customs Information System** (CIS), and we convened two meetings of the CIS Supervision Coordination Group in 2012. In these meetings the Group, in cooperation with the Customs JSA, adopted a joint opinion on the FIDE handbook and an activity report for the preceding two years, while the secretariat presented two draft reports which, upon adoption in 2013, will form the basis of potential follow-up activities of the group in the future.

Moreover, the new **Visa Information System** (VIS) Supervision Coordination Group held its first meeting in November 2012. A database of information including biometric data on visa applications by third country nationals, VIS is 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. Primarily tasked with overseeing the ongoing, gradual roll-out of the system and to facilitate cooperation among Member States, the Group discussed its first working program and shared information on EDPS activities and national inspections in different Member States.

Cooperation in **international fora** continued to attract attention, especially the European and International Conferences of Data Protection and Privacy Commissioners. In 2012, the European Conference was held in Luxembourg and focused on recent developments in the modernisation of the data protection frameworks of the EU, the Council of Europe and the OECD. The International Conference was held in Uruguay on the general theme *Privacy and Technology in Balance*, with a particular emphasis on emerging countries and issues relating to *profiling* and *big data*.

Internal organisation

In 2012, a new sector, IT Policy, was introduced in the organisation, to develop and concentrate our expertise in information technology and data protection. The sector is made up of IT experts with experience in practical IT issues and in policy and supervision. It improves our ability to assess the privacy risks of new technologies, liaise with the technology experts of other data protection authorities and offer guidance on the principles of *privacy by design* and *privacy by default* to data controllers. It also ensures that we can develop our supervision methods and tools in line with technological evolution, in particular with regard to large-scale information systems that are subject to coordinated supervision. The sector will also support the development of a more coherent internal IT policy for the institution.

Resource management

Further to quarterly budget implementation reviews involving the Management Board of the institution, the implementation of our budget increased from 75.66% in 2010, to 90.16% in 2012. New IT tools such as Sysper2 (HR) and MIPs (mission management) have led to increasing efficiency and professionalisation of the EDPS HR function.

Some EDPS key figures in 2012

- ➔ **71 prior check opinions adopted, 11 non prior check opinions**
- ➔ **86 complaints received, 40 admissible**
- ➔ **27 consultations received on administrative measures**
- ➔ **15 on-the-spot inspections and 6 visits carried out**
- ➔ **1 set of Guidelines published** on processing of personal information in the area of leave and flexitime
- ➔ **33 legislative opinions issued** on, among others, initiatives relating to the Area of Freedom, Security and Justice, technological developments, international cooperation, data transfers, public health or internal market.
- ➔ **15 sets of formal comments issued** on, among others, intellectual property rights, civil aviation security, EU criminal policy, the Terrorist Finance Tracking System, energy efficiency, or the Rights and Citizenship Programme.
- ➔ **37 sets of informal comments issued**

1.2. Vision and methodology: the Strategic Review, Rules of Procedure and Annual Management Plan

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

2012 stands out as the year when the institution reached full maturity. This was the result of coordinated processes which came to their conclusion with the adoption of three documents in December: the Report on the Strategic Review, the Rules of Procedure, and the Annual Management Plan.

All three documents are closely integrated. Thus the core values and guiding principles articulated during the Strategic Review are enshrined in Article 15 of the Rules of Procedure. The actions underpinning the new Strategy for 2013-2014 are implemented in the Annual Management Plan for 2013.

All three documents are built on experience and on actions that took place before or during their preparation. Thus input from stakeholders during the Strategic Review process underlined the need to improve our knowledge of IT issues and develop a consistent and authoritative vision on the influence of globalisation and technology on data protection in the EU. In response, as mentioned in the preceding section, the IT Policy sector was created in 2012.

1.2.1 Strategic Review and Strategy 2013-2014

As noted in the 2011 Annual Report, the EDPS launched a strategic review process in July of that year. The process was driven by a number of factors. First, the review was the final stage of a process of internal restructuring begun by the Supervisors in October 2009. The EDPS has developed from a body made up of two Members and a small Secretariat into a fully-fledged institution with almost 50 staff. As part of this process, the Secretariat was restructured in 2010 into an effective institutional form.

Second, after the entry into force of the Lisbon Treaty, the institution entered a phase marked by new challenges, notably the accelerating use of the internet and new technologies, the development of programmes such as the Stockholm Programme and the Digital Agenda, the review of the data protection legislative framework and the implementation of the Lisbon Treaty itself. These developments have caused a marked increase in activities and workload.

Third, resource implications increasingly require the institution to "do more with less". Whilst there has been a slow, steady build up of resources, these do not match the continuing increase over the years in all areas of EDPS activities.

As a result, the strategic review was launched to identify priorities and permit resources to be matched to activities as efficiently and effectively as possible. The process was led by a task force made up of the Director and representatives of all the teams and professional disciplines in the house. The review was concluded in 2012 following an intensive process of internal and external stakeholder consultation. This was carried out by means of internal meetings and an on-line survey of some 500 external stakeholders followed-up by focus groups and interviews.

In general, external stakeholders praised the EDPS as a knowledgeable and authoritative body, providing strong leadership and data protection

expertise. However, they made several suggestions for action, including the need for the EDPS to:

- engage more closely with stakeholders and better understand their policies and institutional constraints,
- work harder to raise awareness of data protection and make it more accessible,
- improve our knowledge of IT issues,
- be selective and focus on areas of high priority or high risk, and to
- support the Data Protection Officers (DPOs) and Data Protection Coordinators/Contact Points (DPCs) who are on the frontline of data protection in the EU institutions and bodies.

This valuable input enabled us to develop our core values and guiding principles and to draw up a detailed plan of actions for achieving our strategic objectives, together with a list of key performance indicators to measure success.

The resulting strategy was adopted in December 2012 in the form of a Report on the Strategy for 2013-2014, *Towards excellence in data protection*. The Report was published on 22 January 2013 and presented to a select group of stakeholders in the EU institutions and the data protection community. The Report and a short video of the proceedings are available on the EDPS website.

Following the suggestions of our stakeholders, we have reassessed our priorities and reallocated our resources, so as to increase our efficiency and effectiveness in a challenging and continuously evolving environment.

From left to right: Peter Hustinx, EDPS, Commission Vice-President Viviane Reding, Commissioner Cecilia Malmström, Giovanni Buttarelli, Assistant Supervisor

Acting selectively and proportionately, we will seek to ensure that data protection is an integral part of policy-making and legislation, in all areas where the EU has competence.

We will focus our attention and efforts on areas of policy or administration that present the highest risk of non-compliance or impact on privacy.

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.

In particular, we have identified activities that emphasise the accountability of policy makers and data controllers and activities that build on the crucial role of DPOs. These activities are key parts of the proposed legislative reforms, and we hope they will show how levels of compliance can be raised in a period of budget restraint.

The Strategy adopted in 2012 is designed to maximise the impact of our work on data protection at EU level and to increase efficiency by making the best use of resources. We will continue to develop the strategy and work towards excellence in data protection at European level beyond 2014.

1.2.2 Rules of Procedure

The Rules of Procedure were also adopted in December 2012, based on Article 46(k) of the Regulation. The adoption of these internal rules constitutes an important step in the maturity of the EDPS as an EU institution.

The Rules of Procedure result from the same process that led to the conclusion of the Strategic Review. They set out in a single, comprehensive document the organisation and working procedures of the institution. They are based on substantial experience and reflect practices that have been developed over the years, in particular following the administrative reorganisation in 2010.

These internal rules complement the rules laid down in the Regulation as well as other provisions of EU law which provide for duties and powers for the EDPS, for example, the Staff Regulations, the Financial Regulation and the various measures dealing with coordinated supervision.

Thus, on the one hand, they recall and apply the principles of independence, good governance and good administrative behaviour and provide for the appointing authority, the authorising officer by delegation and the accounting officer.

On the other hand, they lay down detailed rules concerning internal decision making processes, the roles of the Supervisors and the Management Board, the organisation and working of the Secretariat, planning, internal administration and the openness and transparency of the institution. As noted above, they also enshrine the core values and guiding principles developed during the strategic review process.

The main body of the rules is dedicated to the specific procedures followed when performing the core activities of the institution. Again, some of these procedures are already detailed in the Regulation itself, such as the procedure for prior checking of processing operations, which are complemented by the Rules of Procedure. Other rules were not, or only partly, addressed in the Regulation, such as the rules on cooperation and support of DPOs and the rules on administrative and legislative consultation respectively.

The Rules of Procedure are available on the EDPS website and will be published in the Official Journal in all official EU languages.

1.2.3 Annual Management Plan

Article 13 of the Rules of Procedure provides that, in accordance with the principles of good administration and good financial management, the EDPS shall establish an Annual Management Plan (AMP).

The annual management plan is the foundation for planning activities and managing the workload, complementing and completing the long term strategic planning developed in the Strategic Review and the short term planning followed on a weekly basis. A pilot project was launched in 2012, which showed that, due to the nature of our regulatory and advisory work, not all of our work can be planned. Bound by fixed resources, we have to be able to adapt our planning accordingly. The lessons learned led to the adoption of the first annual management plan for 2013 adopted at the end of 2012.

Following the specific objectives and actions fixed under the Strategy 2013-2014, the annual management plan outlines the activities to be carried out in 2013 under each specific objective. To assess progress towards our objectives we will regularly measure the performance of these activities.

Furthermore, during the Strategic Review process we identified a number of activities which have a key role for the achievement of our goals, and which, therefore, form the basis of the following key performance indicators (KPIs):

1. number of inspections/visits carried out
2. number of awareness-raising and training initiatives within EU institutions and bodies organised or co-organised
3. level of satisfaction of DPOs/DPCs on training and guidance
4. number of EDPS formal and informal opinions provided to the legislator
5. rate of implementation of cases in the policy inventory identified for action
6. number of cases dealt with by the Article 29 Working Party for which the EDPS has provided a substantial written contribution
7. number of cases in which guidance is provided on technological developments
8. number of visits to the EDPS website
9. rate of budget implementation
10. rate of training implementation for EDPS staff

These KPIs will enable us to report on the impact of our work and the efficiency of our use of resources. They will be regularly reviewed and adapted if needed, to improve our future performance. We will include the first set of results in our Annual Activity Report 2013.

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.

Over the course of the year we carried out our main supervision activities, notably in the field of prior checks, complaints and consultations on administrative measures. The prior checking of processing operations which exhibit specific risks remained an important aspect of our supervision work in 2012. Despite a decrease in the number of notifications received, there was a slight increase in the number of opinions adopted (71 opinions, 14 of these being joint opinions covering 44 notifications). Although the number of complaints received also decreased by 20% there was an increase in the number of decisions (26 cases in 2012). Within the framework of consultations on administrative measures, the EDPS 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. In 2012, the EDPS received 27 consultations on administrative measures and provided 23 replies.

Aside from our regular supervision activities, we also developed other forms of monitoring compli-

ance with the Regulation, in line with the Compliance and Enforcement Policy adopted in December 2010. We performed two surveys, one on the status of DPOs in all EU institutions and one on the status of Data Protection Coordinators (DPCs) at the European Commission. The results of these surveys have been compiled in reports, the first of which – on the status of DPOs – was published in December 2012. In addition to these stock taking exercises, targeted monitoring exercises were carried out in cases where, as a result of supervision activities, we had reason to be concerned about the level of compliance in certain institutions or bodies. These took the form of correspondence with the institution or body concerned, one day visits by management to address compliance failings or inspections to verify compliance on specific issues.

We also continued our awareness raising and guidance activities to help promote a data protection culture in the EU institutions. In 2012, this guidance took the form of Guidelines in the area of leave and flexitime, training for DPCs, workshop for controllers, the development of a dedicated area for DPOs in the EDPS website and a helpline for DPOs.

2.2. Data Protection Officers

European Union institutions and bodies have an obligation to appoint at least one data protection officer (DPO) under Article 24.1 of the Regulation. Some institutions have coupled the DPO with an assistant or deputy DPO. The Commission has also appointed a DPO for the European Anti-Fraud Office (OLAF, a Directorate-General of the Commission) in view of its independent functions. A number of institutions have appointed data protection coordinators or contacts (DPCs) in order to coordinate all aspects of data protection within a particular directorate or unit.

In 2012, eleven new DPOs were appointed, both in existing institutions and bodies and new agencies or joint undertakings, bringing the total number of DPOs to 58 (the DPO of the European Central Bank also acts as DPO of the European Systemic Risk Board).

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 has proved to be productive in terms of collaboration and continued throughout 2012.

A 'DPO quartet' composed of four DPOs (those of the Council, the European Parliament, the European Commission and the European Food Safety Agency) was set up with the goal of coordinating a DPO network. The EDPS has collaborated closely with this quartet.

The EDPS attended the DPO meetings held in March 2012 at the European Chemicals Agency (ECHA) in Helsinki and at the European Central Bank in Frankfurt 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 international level, the EDPS Roadmap 2012 which outlines our supervision activity for the year, the DPO status report and the EDPS strategic review. The meetings were also an occasion for open discussions between DPOs and the EDPS on shared issues and common problems such as the conservation of personal information in evaluation procedures.

We organised a number of trainings and workshops for DPOs and DPCs (see section 2.7 Data Protection Guidance) in 2012. In addition, one-to-one sessions took place between EDPS staff and some DPOs on their specific guidance needs.

Colleagues in our Supervision and Enforcement Unit also deal with telephone queries posed by DPOs and whenever possible provide immediate assistance and guidance on specific issues, while leaving more complex issues to be dealt with in written consultations. In the second half of 2012, more than 40 such phone queries were dealt with by staff. In response to the increase in the number of telephone queries, we have put in place a direct helpline for DPOs, with a staff member available to answer questions over the phone at specific times. This initiative has proven useful as it allows us to deal with simple questions in a quick and informal way, strengthening the cooperation and relations between the DPO community and the EDPS.

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 such risks. In 2012, we continued to apply the criteria developed in previous years[5] when interpreting this provision, both when deciding that a notification from a DPO was not subject to prior checking and when advising on the need for prior checking of a consultation (see also Section 2.3.4).

2.3.2. Procedure

2.3.2.1. Notification

Prior checks must be carried out by the EDPS following receipt of an email notification from the DPO to the EDPS Secretariat using the standard EDPS form (Article 19 of the Rules of Procedure). Any additional information relating to the notified processing operation should be provided in an annex to the notification form. If the DPO is in any doubt as to whether a processing operation should be submitted for prior checking, he may consult the EDPS (see Section 2.3.4).

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 checking 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. This phase is coming to an end as we consider that the EU institutions and bodies have been given adequate time to notify their existing processing activities in compliance with Article 27 of the Regulation.

For this reason, we have reminded data controllers to verify that all sensitive processing operations have been notified to the DPO, enabling him or her to in turn notify the EDPS of all outstanding prior checks by the end of June 2013.

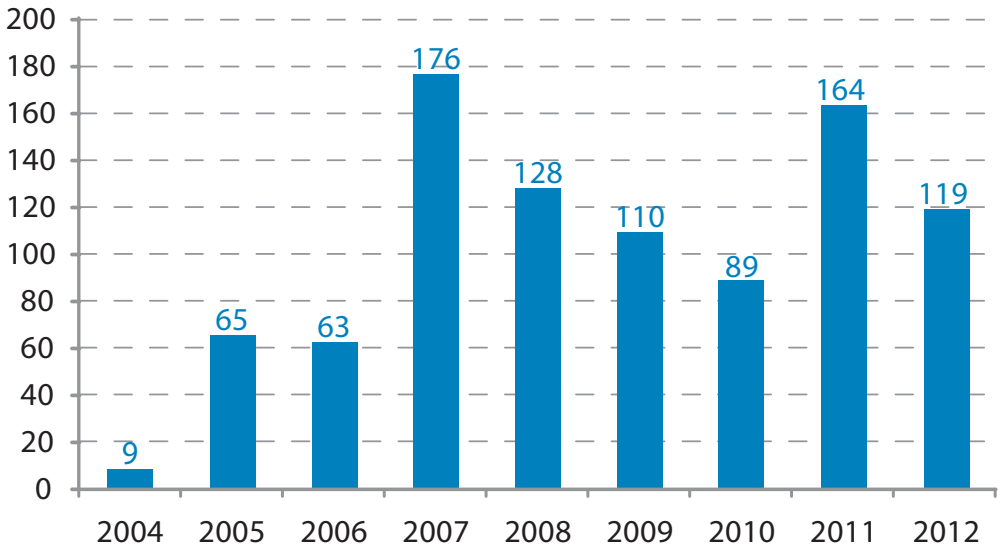
2.3.2.2. Period, suspension and extension

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. 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 months 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 are obliged to send the draft to the institution for feedback on practical aspects and factual inaccuracies which is

5 See Annual Report 2005, section 2.3.1.

Notifications to the EDPS



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).

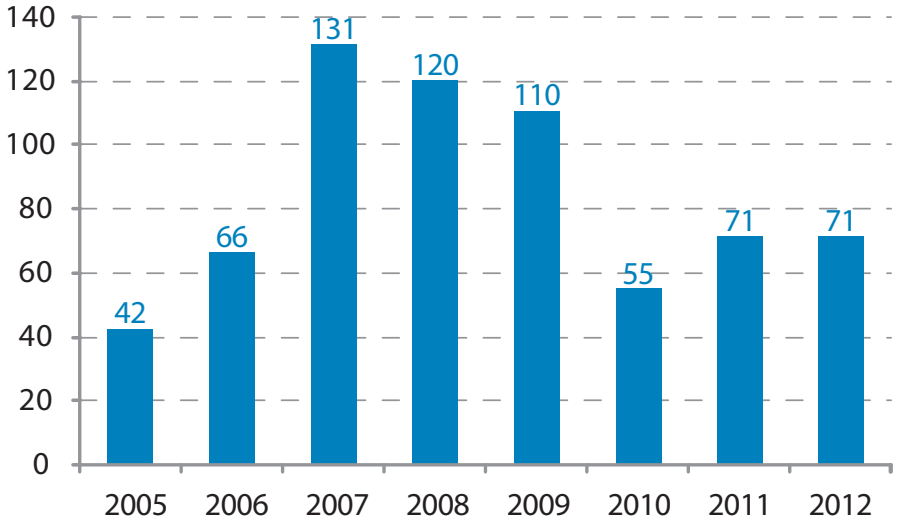
2.3.2.3. Register

In 2012, we received 119 notifications for prior checking (2 were withdrawn). Whilst we have cleared the backlog of *ex-post* prior checks for most EU institutions, processing operations put in place by EU agencies, in particular by newly established ones, the follow-up of Guidelines issued as well as several visits to agencies in 2012 have generated an increase in the number of notifications.

Under the Regulation, we must keep a register of all processing operations for which we have been notified for prior checking (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

EDPS prior-check opinions per year



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 2012, we issued **71 prior checking opinions** and **11 opinions on 'non-prior checks'** (see Section 2.3.5). These figures take into account that we dealt with a significant number of cases by issuing joint opinions: in 2012, we issued 13 joint opinions responding to a total of 41 notifications (see a short explanation of joint opinions in Section 2.3.2.5).

Unlike previous years, when the large EU institutions (European Commission, European Parliament and Council) had been frequent addressees of our opinions, in 2012 we addressed 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 procedures (see Section 2.3.2).

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, recommendations are made so as 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 that 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).

2.3.2.5. Procedure for ex-post *prior checks in EU agencies*

In October 2008, we launched a procedure for *ex-post* prior checks in EU agencies. Since standard administrative procedures are the same in most EU agencies and are typically based on Commission decisions, notifications on a similar theme are gathered and either a collective – or joint – opinion (for various agencies) or a 'mini' prior check opinion addressing only the specific needs of each individual agency is adopted. To help agencies complete their notifications, we summarise the main points and conclusions of previous prior checking opinions on the relevant theme in the form of thematic Guidelines (see Section 2.7).

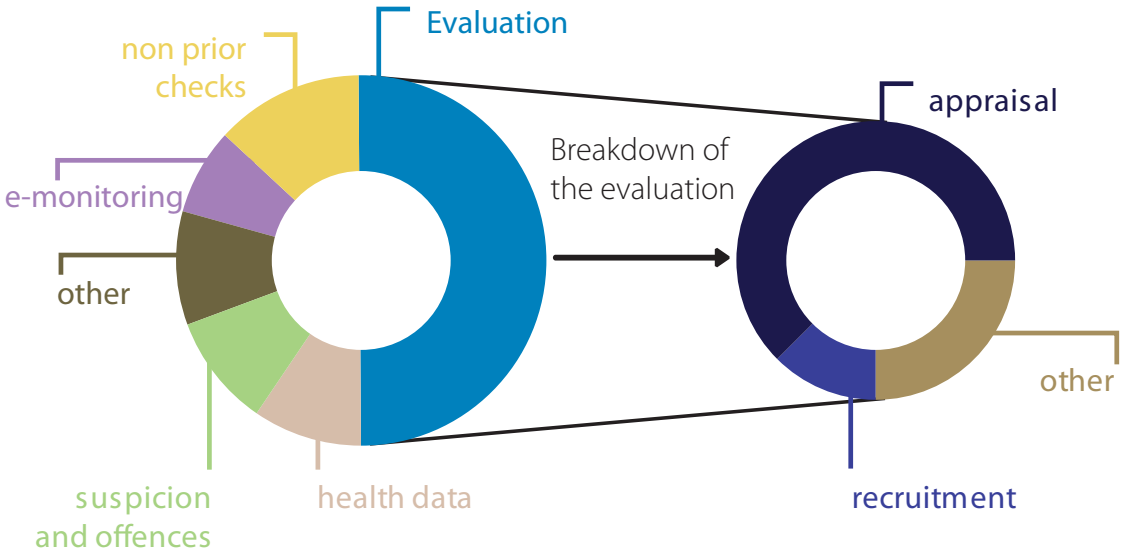
The theme of our first set of Guidelines was **recruitment** and led to us issuing a horizontal opinion in May 2009, covering notifications from 12 agencies. A second set of Guidelines was sent to the agencies at the end of September 2009 on the **processing of health data**, leading to a joint opinion regarding the processing operations of 18 agencies on pre-recruitment examinations, annual check-ups and sick leave absences in February 2011. In April 2010, we issued Guidelines concerning the processing of personal data in **administrative inquiries and disciplinary proceedings** by European institutions and bodies. In June 2011, the EDPS issued a joint opinion covering the processing operations in place at five agencies. Further Guidelines in the area of **anti-harassment procedures** led to the adoption of an opinion in October 2011 covering notifications received by nine agencies.

In July 2011, we published our Guidelines on the **evaluation of statutory staff** in the context of annual appraisals, probation, promotions or regarding certification and attestation. Taking a different approach, we adopted opinions covering evaluation procedures in general per each agency wherever possible. Since publishing these Guidelines, we have adopted 24 opinions (21 of which were in 2012), based on 48 notifications received.

In December 2012, we issued Guidelines on managing the processing of personal information in **leave and flexitime procedures** (on thematic guidance, see Section 2.7).

2.3.3. Main issues in prior checks

Opinions 2012 per main category



2.3.3.1. Processing of personal information in connection with regulations requiring asset freezing as part of Common Foreign and Security Policy (CFSP) related restrictive measures

On 22 February 2012, we issued a prior check opinion on the Commission's processing of personal information as part of restrictive measures in the framework of the Common Foreign and Security Policy. These measures include the **freezing of funds**, of which some measures have been adopted at UN level and some at EU level. The opinion detailed the establishment of a framework for dealing with these measures in the long-term.

To fulfil its tasks under the various legal bases for such measures, the Commission processes the personal information of listed persons and their lawyers. This information is used to correspond with the listed persons, for a review process and for the publication of sanction lists. These lists are published both in the Official Journal of the EU and serve as the basis for a consolidated list, which is published on the Internet.

Our recommendations include **minimising the processing of personal information** to that which is strictly necessary for identifying listed persons, improving the review process and providing better information to the listed persons. In addition, we advised that these recommendations should be applied to future regulations imposing restrictive measures.

2.3.3.2. Revised OLAF investigation procedures

On 3 February 2012, we issued a prior check opinion on the new investigative procedures at OLAF. While the changes were mainly organisational, we referred in general to the recommendations made in our previous opinions on OLAF procedures and put forward some additional specific recommendations. In particular, we advised the controller to:

- strengthen the **protection and safeguards** when dealing with special categories of data in the framework of **investigations**;
- evaluate the **necessity and proportionality** of the current periods for conservation of personal information;
- transmit final reports of internal investigations, especially where no follow-up is recommended, only on the basis of a concrete **evaluation of the necessity of the transfer**;
- put in place an effective mechanism for dealing with the **right to object** or with data protection claims made in the context of inspections, on-the-spot checks or forensic examination of computers.

We also stressed the inevitable privacy risks connected to the forensic examination of computers, where forensic copies of full hard-disks of employee data are made. We therefore requested OLAF to prepare an assessment report concerning the implementation of its relevant Protocol focusing on aspects more strictly related to the processing of personal information in view of a possible revision of the document and current practices.

In the framework of the procedure, it emerged that OLAF intends to set-up a new internal database, the purpose of which is to automatically cross-match new incoming information with information (data fields) extracted from other case files. This analysis would support the procedure for the selection of cases and any subsequent investigation. We found that the new database would need to be autonomously notified and prior-checked in light of its specific characteristics and asked OLAF to suspend the implementation and use of the database until the prior-check had taken place.

2.3.3.3. Safe Mission Data

The purpose of collecting information in the European Parliament's (EP) "Safe Mission Data" system (SMD) is to provide support to EP delegations outside the three main places of work where a rapid and effective reaction is needed in emergency situations.

Our opinion of 24 May 2012 focused on one of the reasons to establish the SMD: the processing of health data to protect the vital interests of the individuals concerned. In principle, the processing of health data is prohibited, but the consent of the individual is one of the exceptions that allows such processing.

We considered that this exception applies to the SMD: the health data processed is provided by individuals on a voluntary basis by means of a collection form, which explicitly notes that there is no obligation to provide any such information. In our opinion we also highlighted the importance of keeping the health data up-to-date and accurate.

2.3.3.4. Organisation of Council meetings of Heads of States or Governments, of Summits or Official Meetings with Third Countries

On 16 March 2012, we issued an opinion on a notification for Prior Checking received from the DPO of the Council of the European Union on the Organisation of Council meetings and meals of the Meetings of Heads of States or Governments, of Summits or Official Meetings with Third Countries and of the Council of the EU and other Meetings at ministerial level or above.

The purpose of collecting personal information for the various meetings is to ensure that participants are served appropriate meals in accordance with their medical and dietary restrictions as well as religious and philosophical beliefs. The purpose for collecting the blood type from the heads of delegations is for medical emergencies.

We considered that the processing of this information is justified so long as the participants voluntarily provide information on their medical, dietary restrictions and blood type. Furthermore, consent

should be based on the information provided by the Council to the individuals on why the information is being requested. The processing of blood type is also justified as it is necessary to protect the vital interests of the individuals concerned.

Finally, we noted that aside from the importance of the privacy statement that the Council should make available to all participants, Council staff members collecting the information should also sign specific declarations of confidentiality.

2.3.3.5. Teleworking – Council of the European Union

On 23 November 2012, we adopted an opinion on a notification for Prior Checking on teleworking received from the DPO of the Council of the European Union.

Although there were doubts as to whether teleworking was subject to prior checking, the processing operation in this case was considered to be subject to prior-checking by the EDPS in view of the evaluation and selection of staff who may be entitled to it (Article 27.2.b). In some other cases, health related data may be processed, which would be another basis for justifying prior-checking by the EDPS (Article 27.2.a).

The purpose of the processing operation in question covered the processing of applications following a call for expressions of interest for teleworking (administrative support to the process of selection of participants) and the administrative follow-up of teleworking. An evaluation in the sense of Article 27.2.b is, therefore, conducted by the data controller.

Our opinion took into account the recommendations made in the pilot teleworking scheme approved by us, namely that the Council should provide all conclusions and modifications which were implemented at the end of the pilot scheme before full deployment of teleworking, that it should consider the personal motivation of the applicants to telework as an evaluation criterion and should only process the information which is necessary for the purpose of teleworking.

2.3.3.6. Annual Declarations of Interest

The European Centre for Disease Prevention and Control (ECDC) notified the EDPS on a procedure established to safeguard its independence from the influence of industry particularly when developing opinions, guidance, advice and recommendations on the emerging threats of infectious diseases to human health.

A system of annual declarations of interest (ADoI) and specific declarations of interest (SDoI) has been put in place for the Members of the Management Board and Advisory Forum, as well as for all experts, seconded national experts and staff members (from AST 5 and above).

In our opinion of 19 July 2012, we recommended that the ECDC carefully consider how it balances the two fundamental rights, privacy and public access to documents, by justifying the need to extend the procedure on declarations of interest (DoI) to all ECDC staff members, to clarify the policy on publishing DoIs and the potentially public nature of personal information collected through SDoIs.

In relation to the publication of ADoIs and the possible public disclosure of SDoIs, we also recommended that the ECDC be proactive, for example, by informing and asking for the consent of the individuals concerned prior to the possible public disclosure of SDoIs in the event of a request and making them aware of their rights under the Data Protection and Public Access regulations.

In its follow up letter, the ECDC justified the use of DoIs for all staff members citing their possible involvement in evaluation committees and scientific panels. With regards to the publication of DoIs, the ECDC policy has been updated and the right to object has been included in the information aimed at those concerned.

2.3.3.7. CEDEFOP internet monitoring (processing of data in connection with a Proxy system)

On 15 November 2012, we issued an opinion on Internet monitoring at the European Centre for the Development of Vocational Training (CEDEFOP).

We welcomed CEDEFOP's methodology for monitoring internet use, which is based on the main pillars of transparency and prior information, a gradual approach to e-monitoring and the rights of staff.

In particular, we were pleased that CEDEFOP has set a general threshold for identifying excessive internet usage and a methodology that enables staff to see the level of their internet usage in real time.

We pointed out some aspects of the processing activities that needed to be modified. Among other recommendations, we advised CEDEFOP to put in place technical safeguards to ensure that the accidental processing of special categories of information (not related to the investigation) is kept to a minimum and occurs only where it is really unavoidable. In such cases, the information should not be recorded or processed further in the subsequent steps of the procedure. Furthermore, CEDEFOP has to inform the users individually, for example by sending the Internet policy document and the privacy statement by e-mail.

2.3.4. Consultations on the need for prior checking

When in doubt, EU institutions and bodies can consult the EDPS on the need for prior checking under Article 27(3) of the Regulation. In 2012, we received 8 such consultations from DPOs.

2.3.4.1. Staff satisfaction survey at the European Agency for Competitiveness and Innovation

The Executive Agency for Competitiveness and Innovation (EACI) submitted a notification relating to its survey on staff satisfaction in the workplace as the processing operations for the study would include an assessment of the hierarchy and EACI by staff which falls within general Article 27.1 of the Regulation.

In our response of 19 October 2012, we concluded that the processing was not subject to prior checking. Furthermore, while the processing of some staff replies to the study could, under other conditions, be considered as processing of personal information related to health, in this specific case, several protective measures (staff not obliged to participate in the study, use of aggregated data for

analysis, publication of general results only, and so on) had been taken.

Nonetheless, we made some recommendations, in order to ensure the correct implementation of the Regulation including some directed at the retention of raw data in the tool used for conducting the satisfaction survey, modifications to the privacy statement, notifying the legal basis of the processing to staff and the method for compiling the aggregated information.

2.3.5. Notifications not subject to prior checking or withdrawn

Following careful analysis, 8 cases were found not to be subject to prior checking in 2012. In these situations (also referred to as 'non-prior checks'), the EDPS may still make recommendations. In addition, two notifications were withdrawn and one replaced.

2.3.5.1. Flexitime and Matrix application at FRA

On 12 April 2012 and 12 September 2012, we concluded that two notifications from the Agency for Fundamental Rights (FRA) were not subject to prior-checking, namely the processing operations in the context of the flexitime and the Matrix applications. These two notifications were connected as the operations are related to the agency's information management system (called Matrix).

We concluded that the case relating to the processing operations on flexitime was not subject to prior checking because the data processing was not intended to evaluate staff efficiency, competence or ability to work. Nonetheless, we made some recommendations so as to ensure full compliance of the data processing with the Regulation. We asked the agency to state more clearly in its procedure that the purpose of the processing operations was not linked to performance appraisal. We also suggested the agency adopt an information notice for staff members and to demonstrate it had been provided to them.

As to the notification on processing operations of the Matrix applications, the EDPS concluded that there was no basis under the Regulation to subject the processing operations taking place within the Matrix application, as notified by the Agency, to a prior-checking procedure. The purpose of the processing operation was not to evaluate individuals but it is to evaluate the project statuses and how the Agency as a whole is progressing in meeting its annual work programme objectives.

The EDPS recommended that the Agency reconsider the necessity of its retention policy for the data stored in the Matrix system. We also recommended that the Agency anonymise the personal data as soon as they are no longer necessary for the purposes of project management in the context of the multi-annual framework and provide the EDPS with the revised conservation period. Finally, the EDPS invited the agency to adopt an information notice for the staff members and to demonstrate it had been provided to the staff.

2.3.5.2. EP Survey work-life balance for women members

The EDPS was consulted on the need to prior check a survey related to the work-life balance for female members of the European Parliament (EP). On 23 October 2012, we concluded that the processing operations concerned would not be subject to prior checking.

The purpose of the data processing was to identify links between work and the personal lives of MEPs and to gather information on what the administration could do to facilitate their work in the EP.

The main basis for prior-checking could have been Article 27.2.a (potential processing of some data relating to health). The conclusion of non-prior checking was based on an analysis of the measures that were taken in order to mitigate the risks outlined in Article 27.2.a of the Regulation. We took into consideration that the purpose of the processing was not to process health related data but to calculate statistical conclusions from aggregated data. Furthermore, a privacy statement informed the MEPS that they were not obliged to take part in the survey, if they did so, they could choose not to answer questions that they did not feel inclined to and no more information than necessary would be processed.

In our recommendations, we suggested that the EP make a distinction between the storage of the individual questionnaires and the aggregated data as the purpose of the processing was to use the information in an aggregated form to deduce statistical conclusions and to implement a very limited retention period for the individual answers. Furthermore, we asked the EP to complete its draft consent form in order for the proposed draft to comply with Articles 11 and 12 of the Regulation.

2.3.6. 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.

Institutions and bodies have chosen to follow our recommendations and to date, there has been no need for executive decisions. In the formal letter that accompanies the opinion, we request that the institution or body concerned informs us of the measures taken to implement our recommendations within a three-month period.

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.

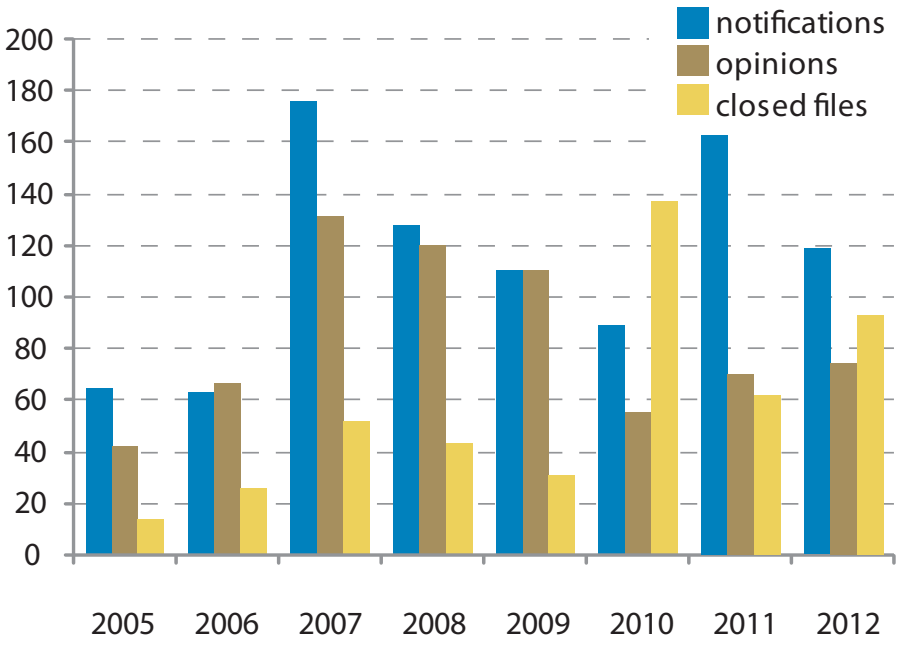
2.3.7. Conclusions

The 71 prior checking 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 the fundamental rights might be put at risk, playing a preventive and precautionary role.

The prior checking cases we handled in 2012 gave us the opportunity to ensure compliance with many of the intrinsic elements of personal data protection, such as data minimisation, privacy by design, pro-

Comparative situation



portionality, and so on. We will continue to provide such guidance to institutions and agencies and to facilitate the notification process from agencies.

In terms of follow-up of our prior checking opinions, we closed 92 cases in 2012. 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 if the complaint is 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 and anonymous requests are therefore not considered. However, anonymous information may be taken into account in the framework of another procedure (such as a self-initiated enquiry, or a request to send notification of a data processing operation, etc).

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 manager of a research institute, who contributed to a research project managed by one of the EU institutions, complained about the outcome of an audit on the project. The audit service of the institution which financed the project considered some of the complainant's expenses unjustified and requested their reimbursement. During the audit some personal information was processed by the auditors and the complainant considered that the audit was illegal given that the data subjects did not give consent for the processing of their personal information. The EDPS did not follow the reasoning of the complainant as the processing of personal information during an audit has another legal basis than the data subject's consent. Therefore, no inquiry on the complaint was initiated in this case.

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 British citizen complained to the EDPS about the refusal of the Austrian Data Protection Authority (DPA) to deal with his complaint in English instead of German. The complainant asked the EDPS to instruct the Austrian DPA to handle his complaint in English or to translate the complaint and its annexes into German. We advised the complainant that the EDPS is not competent to supervise national DPAs and is not in a position to provide translation services to citizens who face language barriers whilst exercising their rights in different Member States.

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 our process of submitting complaints by offering an interactive **online complaint submission form** on our website. This form helps complainants to assess the admissibility of their complaint and thereby submit only relevant matters to the EDPS. It also allows us to analyse more complete and relevant information in order to speed up the processing of complaints and to reduce the number of manifestly inadmissible complaints. The form is available in English, French and German. As of September 2011, if a complaint is received by e-mail in one of these languages, the complainant is invited to fill in the online form. This measure has reduced the number of inadmissible complaints received in 2012 by approximately 38%.

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. This manual was updated in September 2011 in order to reflect changes in our organisational structure and to integrate recent developments in the practice of complaint handling. 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 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.

An EU citizen was informed that his personal information appeared on a list managed by an EU institution of persons and businesses excluded from taking part in public tender procedures. He complained to the EDPS about not being informed by the institution of the reasons to include him on this list. We advised him that his complaint to us could only be admissible if the institution processing his personal information had not responded to a specific request from him. He should, therefore, first approach the institution concerned with his request and approach the EDPS only if access to information is not granted within a deadline established by data protection rules.

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.

A staff member of an EU institution complained to the EDPS about a transfer of his medical reports to other staff members in the context of an administrative procedure. After the EDPS had begun his inquiry into the complaint, the complainant initiated a case before the Civil Service Tribunal of the EU based in part on the same facts. The EDPS decided to suspend his inquiry until the judgment was delivered by the Tribunal. Given the seriousness of the alleged breach of the data protection rules, the EDPS decided to intervene before the Tribunal in support of the complainant.

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 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 opinion 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 2012.

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 Data Protection Officer (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. We may publish information about the complaint on our website or annual report in a form which does not allow the complainant or others involved to be identified.

2.4.4. Complaints dealt with in 2012

2.4.4.1. Number of complaints

In 2012, the EDPS received **86** complaints (a **decrease** of approximately 20% compared to 2011, confirming the effectiveness of the **online complaint submission form** available on our website in reducing the number of inadmissible complaints). Of these, 46 complaints were **inadmissible** *prima facie*, the majority relating to processing at national level as opposed to processing by an EU institution or body.

The remaining 40 complaints required in-depth inquiry (an increase of about 54% compared to 2011). In addition, 15 admissible complaints, submitted in previous years (four in 2009, three in 2010 and eight in 2011), were still in the inquiry, review or follow-up phase on 31 December 2012.

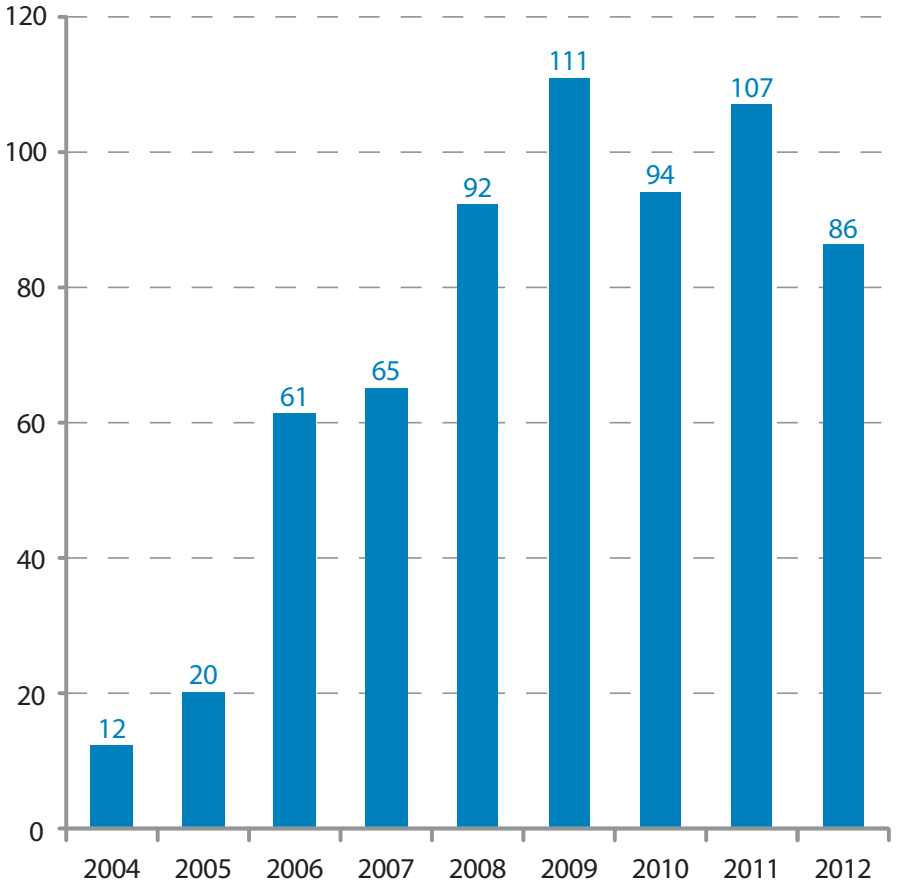
2.4.4.2. Nature of complainants

Of the 86 complaints received, 20 complaints (23%) 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 66 complaints.

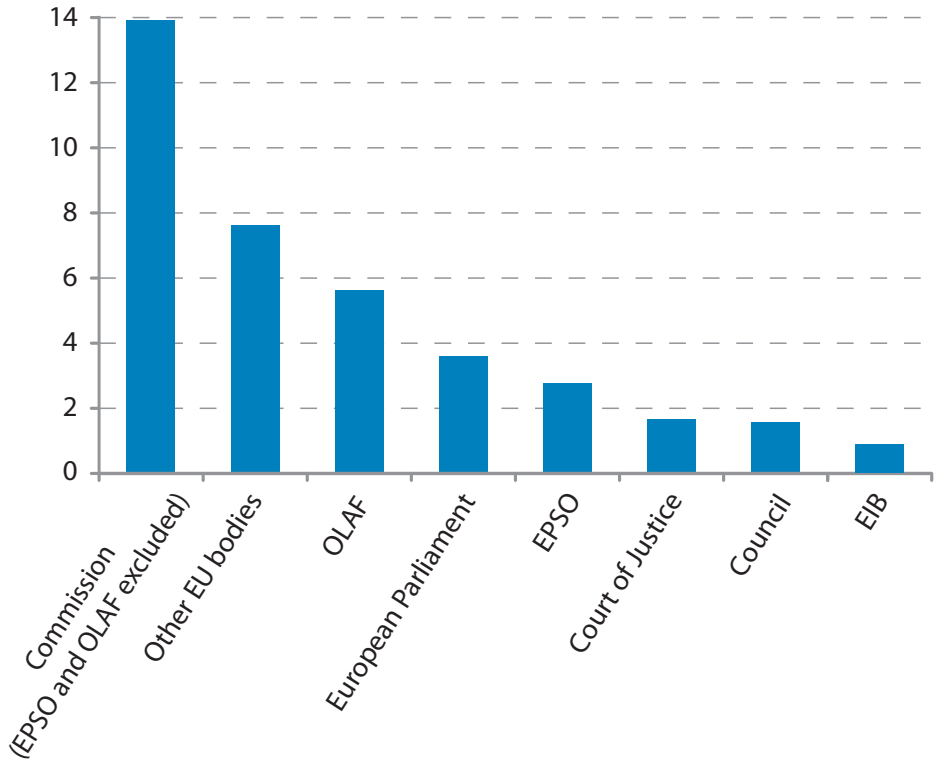
2.4.4.3. Institutions & number of complaints

Of the 40 admissible complaints submitted in 2012, most were directed against the **European Commission, OLAF,** the **European Parliament and EPSO**. 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 related to OLAF and EPSO may be explained by the nature of the activities undertaken by those bodies.

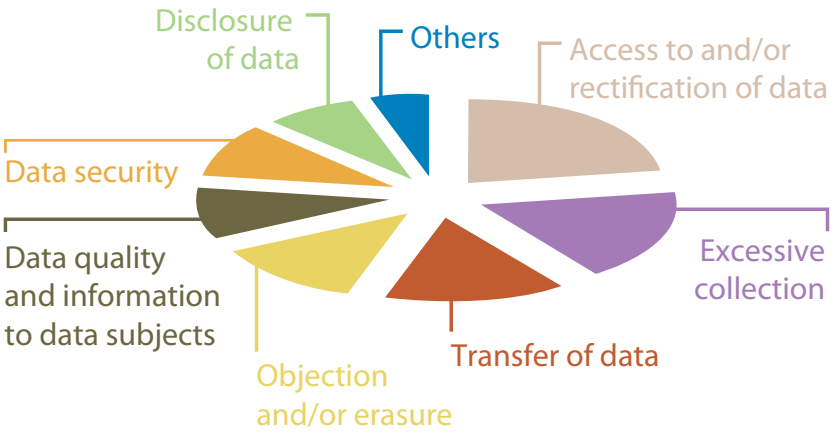
Number of complaints received



EU institutions and bodies concerned



Types of violations alleged



2.4.4.4. Language of complaints

The majority of complaints were submitted in English (69%), French (13%) and German (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 2012 related mainly to:

- A breach of data subjects' rights, such as access to and/or rectification of data (23%) or objection and/or erasure (13%);
- Excessive collection of personal information (18%), transfer of data (15%), data quality and information to data subjects (10%), data security (10%) or disclosure of data (8%).

2.4.4.6. Results of EDPS inquiries

In 26 cases resolved during 2012, 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.

The EDPS received a complaint relating to some files of the Staff Committee of an EU body being freely accessible to all staff members. The EDPS concluded that there was no evidence of significant violation of the data protection rules which would justify further inquiry in this case. Therefore the EDPS closed the case.

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

A complaint was received alleging that an EU body communicated the name of an informant, who was a member of staff of an EU institution, to his hierarchy. Following an inquiry into the matter, the EDPS concluded that the disclosure of the informant's identity constituted an unauthorised disclosure of the personal information in breach of Article 22 of the Regulation.

In one case, allegations reported to the EDPS in the context of a complaint led to his decision to launch a broader, on-the-spot inspection at 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 by 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. These took the form of a one day **visit** to the body concerned with the aim of addressing the compliance failings. Finally, **inspections** were carried out in certain institutions and bodies to verify compliance on specific issues.*

2.5.1. General monitoring and reporting: Report on the Status of Data Protection Officers and Survey on the function of Data Protection Coordinator

In our policy paper of December 2010, the EDPS announced that "*he will continue to conduct periodic "surveys" in order to ensure that he has a representative view of data protection compliance within EU institutions/bodies and to enable him to set appropriate internal objectives to address his findings*".

We have been a firm supporter of the DPO function in the EU administration. Thus, in May 2012, we launched a survey dedicated to the Data Protection Officer (DPO) in order to monitor the compliance of EU institutions and bodies with Article 24 of the Regulation. The importance of the DPO function has also been recognised in the package for reforming the EU rules on data protection, currently under discussion by the EU legislator.

In the form of a questionnaire, the survey focused on the mandate, position and resources (time, support and training) of the DPO so as to collect consistent information about the state and evolution of the DPO function. The conclusions of this exercise were compiled in a report. The responses were displayed in three tables, by groups of institutions and bodies to allow comparison.

In the conclusions, we welcomed the designation of a DPO by almost all EU institutions and bodies, the general compliance with a term of office between two and five years, the experience already achieved within the DPO network, the administrative attachment of the majority of the DPOs to the Head of the institution or body and the existence of significant support staff for many DPOs.

On the other hand, the report also reveals several areas of concern. In particular, we will closely monitor the actual duration of the mandate of those DPOs who are contract staff, the high DPO turnover, the possible conflicts of interest, particularly for part-time DPOs attached to the administration. Where appropriate, we will address such issues on a case by case basis.

Furthermore, we will take into account the conclusions of this exercise when planning future supervision and enforcement activities. The report on the status of DPOs was published in December 2012.

In June 2012, we launched a survey on the function of Data Protection Coordinator (DPC) at the European Commission. In the form of a questionnaire, the survey will form part of a wider project concerning the function of the DPC in all EU institutions or services that have set up a DPC network. Information gathered through this general survey will then be used to draft a paper on the DPC function in EU institutions. The results of the survey will be drafted as a report, to be issued in 2013.

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 just 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.

Between January and December 2012, we visited six EU agencies: REA, ERCEA, ETF, EASA, ECDC and Frontex.

The results of the visits can be measured in terms of raising awareness of data protection; raising the level of compliance via commitment of the management; increasing our knowledge of agencies and, in general, fostering better cooperation with the agencies visited. ETF in particular demonstrated active cooperation with us in adopting concrete measures to implement recommendations agreed in the road map.

As part of the effort to raise awareness on compliance with the data protection rules and engaging the commitment of management, Giovanni Buttarelli, Assistant EDPS, attended the meeting of the Heads of Agencies in Stockholm in October 2012. He presented the main principles of the new draft data protection regulation – such as accountability, reduction of administrative burden, transparency, security and effective supervision and enforcement

– to underline the need to anticipate the integration of these concepts in EU agencies. He also stressed the value of the DPO role, insisting on the importance of supporting the DPO. Mr. Buttarelli also used the occasion to present our new policy on consultations in the field of supervision and enforcement (see Section 2.6.1).

2.5.3. Inspections

Inspections are another important tool that enable the EDPS to monitor and ensure the application of the Regulation. They are provided for under 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.

During 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 2012, we continued the follow-up of previous inspections. In addition, we inspected EURODAC and OHIM in February and April respectively. Targeted, on-the-spot inspections were conducted in June and July at thirteen Brussels-based EU institutions and bodies on the way they inform the general public about video-surveillance on their premises.

Follow up of the inspection at the Joint Research Centre – European Commission

We carried out an on-the-spot inspection at the Joint Research Centre (JRC) in Ispra at the end of 2010. The corresponding inspection report outlined the selection and recruitment of JRC personnel and highlighted serious deficiencies in the different procedures put in place by the security service (pre-employment security check, security investigations, access control and recording of emergency calls). In 2012, we monitored the implementation of our recommendations via quarterly reports from the JRC. The fourth and final report was received from the JRC after summer 2012.

The part of the inspection report related to selection and recruitment of JRC personnel was closed at the end of 2012 while our recommendations on the security issues analysed led to the abolition of a security screening procedure by the European Commission. It also led to the adoption of a new set of security rules. The notifications for these new security procedures were sent to us in December 2012 and will be analysed in 2013.

Follow-up to the security audit of the central unit of the Visa Information System

In November 2011, we carried out a security audit of the central unit of the Visa Information System (VIS). This audit assessed if the physical infrastructure, personnel, organisation and IT technologies complied with the security requirements provided for in the applicable legislation and also in the Commission Decision 260/2010 on the Security Plan for the operation of the system.

Although no critical security problems were found that would have justified imposing a temporary ban on processing, we identified several important security risks and outlined them in our report of June 2012. As a consequence of these risks, we requested that immediate action be taken by the Management Authority.

We received appropriate follow-up reports from the European Commission. Substantial progress had been made in meeting the recommendations of the security audit, however, several issues remained open at the time of hand-over to the new EU agency for large-scale IT systems. This agency became operational on 1 December 2012.

Inspection at EURODAC

In February 2012, we carried out a second inspection of EURODAC. The scope of this follow-up inspection was to verify implementation of our recommendations from the first inspection in 2006 and the security audit of 2007, as well as to assess the overall organisational and technical procedures in place to protect personal information and security in EURODAC plus.

Our inspection included a security audit and covered the information systems of the operational Central Unit (CU) and the backup site (BCU). The overall data processing operations performed by the EURODAC Central Unit were considered at application, database and server level and relevant organisational, technical and physical security measures were assessed.

We found the overall level of data protection and security of the EURODAC Central Unit to be high. The provisions of the EURODAC Regulation with regard to the data processing are being respected (types of information recorded, data retention periods, specific requirements for advance deletion and blocking of data, etc). A specific security policy is being followed, clearly defining the roles and responsibilities of the EURODAC management team and including detailed procedures for several aspects of IT security.

A number of technical security measures have been implemented to safeguard personal information at application, database and server levels. Strong physical security measures are in place in all EURODAC locations. Most of our recommendations from the 2006-2007 inspection and security audit have been taken into account in EURODAC plus.

Inspection at the OHIM

In April 2012, we inspected the Office of Harmonization for the Internal Market (OHIM) in order to raise awareness about the EDPS, our powers and the importance of compliance with data protection rules. The OHIM was selected for inspection on the basis of a risk assessment exercise – the OHIM scored below one of the benchmarks established in its peer group in the 2011 EDPS Survey. The overall aim of the inspection was to verify facts and practices particularly as a follow-up to specific complaints and to check the full implementation of our recommendations in a number of prior check opinions.

The OHIM cooperated fully and constructively throughout our inspection. Following a comprehensive examination of the evidence gathered, we issued a number of recommendations. The OHIM implemented these swiftly, allowing us to close this case in November 2012.

Targeted CCTV inspection

On 14 November 2012, we adopted a report on the findings of some on-the-spot inspections conducted between 15 June and 18 July 2012 on the premises of thirteen Brussels-based EU institutions and bodies. These thematic inspections were one of the measures announced in our Follow-up Report of February 2012 on the status of compliance of EU institutions and bodies with our 2010 Video-surveillance Guidelines.

Based on our findings, our recommendations to the EU institutions and bodies inspected on how to better inform the general public about video-surveillance included:

- the placing, location and content of an on-the-spot notice (a pictogramme accompanied with some basic information) highlighting that the area is under surveillance;
- a more comprehensive data protection notice summarising the why and how of the video-surveillance, an outline of the safeguards and how individuals can exercise their rights;
- an online policy on video-surveillance detailing the approach of the EU institution or body concerned.

The feedback of the EU institutions and bodies inspected is currently being examined.

2.6. Consultations on administrative measures

2.6.1. Consultations under Articles 28.1 and 46(d)

On 23 November 2012, we issued 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 explained in the policy paper, we encourage controllers to submit consultations to us in the specific, limited cases when the matter presents either: (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, due to the extension of the measure, etc.). In principle, the EDPS shall 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).

Within the framework of consultations on administrative measures envisaged by an institution or body, a variety of issues were examined in 2012, some of which are reported below.

2.6.1.1. Billing individual users of fixed phone calls made for non-work related purposes – EFSA

On 1 March 2012, we replied to a consultation on an EFSA policy for billing individual users of fixed phone calls made for non-work related purposes.

Firstly, we addressed the issue of whether this EFSA policy had to be notified to the EDPS for prior checking. We highlighted that a distinction must be drawn between the processing of information solely for billing and traffic management without any assessment of the individual conduct, on the one hand, and the processing of information with a view to monitoring and assessing individual conduct on the other (for instance for detecting excessive or unauthorised use of telephone by staff). While the former processing type is not subject to prior checking as such, the latter is. Although the written policy of EFSA referred to the verifying of authorised use of telecommunication systems, the EFSA DPO clarified that the sole purposes of the policy are billing and budget management and thus proposed removal of the reference.

We considered that some of the categories of information included in the template invoice sent by the telecommunications company were not necessary for the purpose of billing. In particular, we suggested that the fields relating to the identification of called persons and unanswered calls be removed from the invoice.

We also recommended that EFSA limit the number of people authorised to access to the data and remind those authorised persons that the sole purpose of the data is for billing and budget management. Finally, EFSA should provide current and future staff with adequate information pursuant to Articles 11 or 12 of the Regulation.

2.6.1.2. Internet publication of the official directory of agents of European institutions and bodies

The publication by a European Union institution or body of names, tasks and contact details of civil servants on their institutional websites involves the processing of personal information by that institution or body and is thus subject to the Regulation. Accordingly, the publication of this information must be based on one of the grounds for processing pursuant to Article 5 of the Regulation.

In our opinion of 8 February 2012, we considered that the publication of a directory of staff can be based on Article 5(a) of the Regulation as it is done in the public interest, i.e. to increase accessibility and transparency in line with Articles 1 TEU and 15 TFEU. It is, however, for the institution or body concerned to evaluate, on a case by case basis or per categories of staff, whether such publication is necessary in specific cases and which information needs to be published (by reason, for instance, of the staff member functions, responsibilities, frequent relationships with external stakeholders, etc.).

In order to reinforce and clarify the legal basis for the processing, we recommended that the institution or body concerned should adopt a decision or another administrative act describing the purpose, the conditions and the modalities for the publication as well as other relevant characteristics of the directory.

Current and future staff should be provided with clear and comprehensive information in compliance with the Regulation (Articles 11 and 12) and granted the right to object to the publication on compelling and legitimate grounds (Article 18). Moreover, the institution or body concerned should take all the necessary measures to prevent personal information contained in the directory from being used for direct marketing, spamming or other malicious purposes (see Article 38(2)).

2.6.1.3. EACI: only relevant certificates should be collected for indefinite contracts

We received a consultation from the DPO of the European Agency for Competitiveness and Innovation (EACI) under Article 46(d) of Regulation 45/2001 on the collection of CAST certificates from all contract agents (CA) working at the EACI.

The purpose for processing CAST certificates is to complete and update CA personnel files, as it is a requirement in order to benefit from an indefinite contract within the EACI. In our reply of 23 July 2012, we considered that the processing is generally in line with the Regulation.

However, we noted that EACI's HR also asks staff members to provide CAST certificates which relate to a different function group than the one they have been recruited for at the EACI and for which they would benefit from an indefinite contract. In this particular case, we highlighted that CAST certificates cannot be considered relevant to the new purpose and recommended that the HR only collects the CAST certificates which are relevant to the function group for which staff members have been recruited.

2.6.1.4. Consultation on the OLAF revised Model Data Protection Contractual Clauses to be used in Administrative Cooperation Agreements concluded with third country authorities or international organisations

In our opinions of 3 April and 16 July 2012, we recognised that the European Anti-Fraud Office's (OLAF) potential to share information with third country authorities and international organisations is an important element in combating international fraud. Nevertheless, any exchange of personal information has to be in conformity with the existing legal framework governing trans-border transfers of personal data by EU institutions and bodies, namely Article 9 of the Regulation.

We urged OLAF to reinforce the substantive safeguards, compliance and redress mechanisms in place. Among other things, we recommended that:

- OLAF should carefully select its partners and make a preliminary assessment of their capacity and willingness to respect the clauses of the **Administrative Cooperation Agreements** (ACAs) and its annexes;
- OLAF should put in place the necessary measures to verify, to the extent possible, the correct implementation of the agreement by its ACA partners and periodically report to the EDPS;
- Should a problem arise, OLAF and its partners should do their best to find a solution, including where appropriate and necessary, make specific concessions to data subjects.

2.6.1.5. Transfer of medical data of pre-recruitment candidates between the medical services of institutions

Following the CST judgment in Case F-46/09, V v. EP, DG HR of the Commission submitted a consulta-

tion under Article 28.1 of the Regulation concerning the transfer of medical data of pre-recruitment candidates between the medical services of institutions. They submitted a draft conclusion to be approved by the College of Heads of Administration (CCA), an explanatory note to the draft conclusion, a draft consent form and a privacy statement.

We identified three areas to be analysed.

- As regards the *lawfulness of the processing*, we clarified that the processing cannot be based exclusively on consent, since consent is a weak legal basis in the context of employment and it should, therefore, be considered a supplementary guarantee of the transfer. We recommended that the Commission clearly indicate that the internal rules are the main legal basis, as required in Article 5(a) of Regulation 45/2001.

- As to the principle of *necessity*, the Commission highlighted "useful" reasons for justifying the transfer of data: avoiding a second check-up by another institution reduces expenses, accelerates the procedure and reduces fraud. We referred to the judgment in V v. EP (paragraph 131) which strengthened the principle of necessity by using the term "indispensable". We recommended that the Commission provide reasons that make a transfer necessary and indispensable in light of Article 7 of the Regulation and erase any reference to mere "utility".

- With regard to *consent and the right to withdraw*, the Commission included an opt-in mechanism. However, we suggested the Commission specify that data subjects may withdraw their consent at any time rather than within 10 days, indicate that data subjects can refuse to give their consent without prejudice to their rights and those data subjects who refuse to give consent should not be suspected of fraud.

On following-up this consultation, we found that the Commission adopted adequate measures implementing our recommendations. The Commission will thus submit its draft conclusion to the CCA for approval, so that in the interests of harmonisation, the EU institutions and bodies can adopt the same internal rules.

2.7. Data protection guidance

The experience gathered in the application of the Data Protection Regulation has enabled us to translate our expertise into generic guidance for institutions and bodies. In 2012, this took the form of follow-up to previous guidance to institutions in the areas of leave and flexitime, training for DPCs, workshops for controllers, a dedicated area for DPOs on the EDPS website and a telephone helpline for DPOs.

We are currently working on Guidelines for absences and leave, procurement and selection of experts, e-monitoring and data transfers.

2.7.1. Thematic Guidelines

Follow-up Report on Video-Surveillance

In February 2012, we issued our Follow-up Report outlining the status of compliance of European institutions and bodies with the Video-Surveillance Guidelines issued by the EDPS in March 2010.

This Follow-up Report presents a systematic and comparative analysis of the state-of-play reports received from a total of 42 EU institutions and bodies. As a result, we were reassured that the Guidelines contributed to raising the level of awareness and transparency in video-surveillance matters within the bodies.

We took note of the considerable efforts undertaken by those institutions and bodies which submitted their state-of-play reports, particularly in terms of overall participation levels, the limited use of "intrusive" CCTV and "privacy by design" approaches.

At the same time, we were disappointed that almost two years after the adoption of the Guidelines and more than two years after starting the consultation process, the implementation of the Guidelines has been put on hold or significantly delayed in several institutions. This involves matters such as the content of on-the-spot notices, the publication of online video-surveillance policy documents, a lack of impact assessments as well as insufficient data protection training.

Apart from applauding best practices, our Follow-up Report highlights the shortcomings of those institutions lagging behind in their efforts to ensure compliance with the Guidelines and announces follow-up measures.

Guidelines concerning the processing of personal data in the area of leave and flexitime

In December 2012, we issued Guidelines on managing the processing of personal information in leave and flexitime procedures.

The Guidelines cover the processing of personal information in the management of all sick leave, annual leave and all forms of special leave entitlements related to the working conditions of officials,

temporary agents, contract agents and seconded national experts. The Guidelines also include an analysis of the flexitime time management system processing operations.

The objective of the Guidelines is to offer practical guidance and assistance to all DPOs and controllers in their task of notifying existing and/or future data processing operations to us. The DPO network was consulted on the draft in October 2012. The Guidelines should serve as a basis for notification for institutions and bodies which have not notified their procedures and as a practical guide for all institutions and bodies.

Regarding leave processing operations, we insist on the obligation of confidentiality imposed on the persons in charge of processing health related data (special categories of data) as well as to ensure the quality of the data being processed. Another important aspect which requires special attention is the retention periods for leave related information.

For flexitime processing operations, we offer examples of cases for which prior checking notification is not necessary and also for those cases where such notification is required. In addition, we insist on the data subject's right of access and right of rectification. Finally, we analyse the potential to link information from time management systems to other systems.

2.7.2. Training and workshops

Two workshops for Data Protection Coordinators (DPCs) were organised by the EDPS on 14 June and 20 September 2012 in Brussels. Welcoming DPCs from 7 institutions (Commission, European Parliament, Council, European Central Bank, European Investment Bank, European External Action Service, Court of Auditors), both events were well attended by 42 and 13 participants respectively. There were presentations from DPOs as well as from EDPS Supervision team colleagues, giving a good flavour of both theory and best practice. The workshops were well appreciated by DPCs, with comments highlighting the useful exchanges with colleagues, counterparts from other institutions and EDPS staff.

Following the publication of our Guidelines on evaluation[6] and related prior checking opinions in which we reconsidered the conservation periods of evaluation data, we hosted a workshop on the conservation of data in evaluations on 4 December 2012. Participants of the workshop, held in our new premises, included representatives of HR and document management officers, DPOs from the three main institutions, the ECB, the executive agencies and EDPS colleagues. The aim of this workshop was to foster discussion on the existing conservation periods for evaluation data in personnel files and the data protection rules related to it. We hoped to better understand the needs of the EU administration and determine conservation periods of documents collected and processed in this context.

In conclusion, participants agreed that a survey to gather information (detailed examples) on the administration's needs in relation to the conservation of specific categories of documents should be circulated. Once finalised, it should be sent to all DPOs for dissemination to relevant departments for further input. The information gathered could be the basis for developing a proposal of appropriate conservation periods for specific categories of documents.

2.7.3. DPO Corner and other tools

As announced in our Annual Report 2011, we launched the DPO corner of the EDPS website in July 2012. This 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 informative documents on the role and missions of the DPOs, a variety of templates and presentations to help DPOs in their awareness raising activities, summaries of recent developments in the data protection arena, and an events list (training courses or meetings). This information is updated on a regular basis.

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

[6] The Guidelines are available on EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/11-07-15_Evaluation_Guidelines_EN.pdf

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

2012 was a year of major developments in the field of data protection. The Commission continued to publish a large number of legislative proposals affecting data protection, with a comprehensive reform of the existing data protection rules as the main theme. This project featured high on the EDPS agenda in 2012 and will remain so as the legislative procedure advances; the previous and ongoing discussions in the European Parliament and the Council have generated increasing interest in this reform from a multitude of public and private sector stakeholders, from both within and outside the EU. The process has also demonstrated a fundamental understanding of the underlying principles of the reform by the EU institutions.

Following the trend of past years, the areas covered by EDPS opinions has continued to diversify. Aside from traditional priorities, such as the further development of the Area of Freedom, Security and Justice (AFSJ) or international data transfers, new fields are emerging. A number of opinions in 2012 focused on the digital market and consumer safety in the online environment. Among those, the topics of personal health data and personal credit information stood out.

In 2012, we also published an opinion on **cloud computing** to emphasise data protection principles and the importance of their correct implementation in this prominent phenomenon. In it, we detailed and justified the necessary standards for data protection in the cloud. Such opinions are intended to provide guidance and become benchmark references for upcoming hot topics and data protection issues.

The progressing **interoperability** of sophisticated **consumer technology** and the **internet** (smart devices for instance) presented new challenges in

limiting the processing of personal information to the purposes for which it was collected. Access to restricted information or utilising formerly irrelevant or inaccessible data for new purposes has been at the core of some of our recent work. The opinion on smart meters, devices which can enable significant energy savings yet potentially also imply a form of domestic surveillance, is an example of a proposal we commented on that illustrates this trend.

In the **AFSJ**, the question of necessity has been a recurrent theme. We have issued several opinions in which this data protection principle figured prominently. This was the case for our opinion on EURODAC[7], SIS II[8] and the European Cybercrime Centre[9]. We are acutely aware of the trend for law enforcement agencies to argue for increased access to other databases, such as those used by customs and immigration, for crime prevention purposes.

Opinions related to the **internal market** also continued to feature prominently in 2012 with an additional emphasis on the digital market. We adopted, amongst others, a package of four opinions in the field of the financial market regulation[10].

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, the basic approach for 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 the 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 aspects 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 data protection is a core element. 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) of the European Parliament or in the relevant working parties of the Council.

A recent addition to these instruments is the publication of *prospective opinions*. We use these to explain the importance and utility of the correct implementation of data protection principles. Prepared on our own initiative, they are not linked to a specific legal proposal. Rather, they are intended to provide guidance and serve as a future benchmark reference for fundamental data protection issues and principles.

Consultations with the Commission take place at various stages in the preparation of proposals, and the frequency varies depending on the subject and on the approach followed by the Commission services. This is particularly so for long-term projects, such as the reform of the legal framework for OLAF, to which we have contributed at different junctures.

Formal consultation activities are quite often preceded by 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

7 See section 3.4.6.
8 See section 3.4.4.
9 See section 3.4.3.
10 See section 3.5.3.

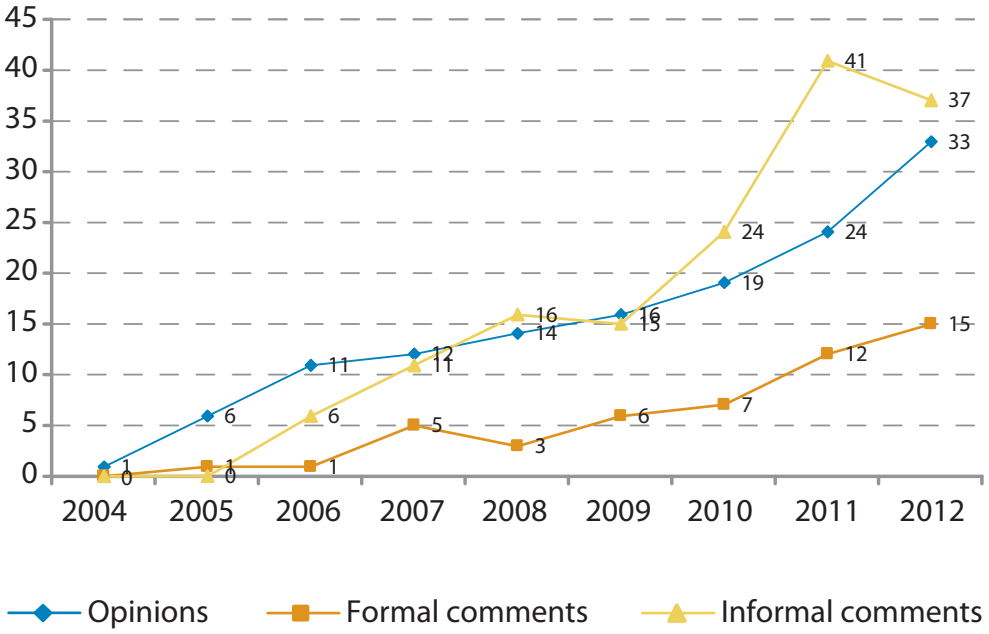
stage, i.e. before the proposal is finalised and adopted. These informal comments, of which there were 37 in 2012, allow data protection issues to be addressed at an early stage when the text of a proposal can still be changed relatively easily. The submission of informal comments to the Commission is 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 2012

In 2012, there was a steady increase in the number of opinions we issued. We issued 33 opinions, 15 formal comments and 37 informal comments on a variety of subjects. With these and other interventions, we implemented our priorities for 2012, as outlined in our inventory.

Legislative opinions evolution 2004-2012



3.3. Review of the EU Data Protection Framework

The major legislative project of 2012 for the EDPS was, without doubt, the data protection reform package. We have underlined the need for updated and stronger EU rules on data protection on numerous occasions and on 25 January, the Commission adopted its reform package, comprising two legislative proposals: a general Regulation on data protection and a specific Directive on data protection in the area of police and justice.

Our first reaction was to welcome the general Regulation as a huge step forward for data protection in Europe, an excellent starting point for the adoption of European rules on data protection, robust enough to face future information technology-driven challenges.

However, with regard to the Directive, we were very critical of its inadequate content. We pointed out that the Commission had not lived up to its promises to ensure a robust system for data protection in the areas of police and justice and questioned why the Commission excluded the area

Peter Hustinx, EDPS, meets Sabine Leutheusser-Schnarrenberger, the German Federal Minister of Justice

from its original intention of proposing a comprehensive legislative framework.

On 7 March, we adopted an opinion elaborating our position on both proposals in greater detail. In a public statement, the EDPS concluded that the two legislative proposals would still leave Europe far removed from a comprehensive set of data protection rules – both at national and EU level – in all areas of EU policy. This is especially so because the proposals leave many existing EU data protection instruments untouched, such as the data protection rules for the EU institutions and bodies as well as specific law enforcement instruments.

One specific improvement of the proposed Directive was welcomed, namely that the proposal also covers domestic processing. However, we emphasised that this would only have added value if the Directive substantially increased the level of data protection in this area, which is not the case.

We highlighted that the proposed data protection rules for law enforcement were unacceptably weak. We noted many instances where departing from the rules provided for in the proposed Regulation was not justified. We pointed out that specific rules are needed for law enforcement, but not a general lowering of the level of data protection.

We also expressed particular concerns with regard to:

- the lack of legal certainty about the further use of personal information by law enforcement authorities;

Our opinion on the review of the EU Data Protection framework underlined several positive points of the Regulation:

- the rules will be directly applicable in Member States;
- they will do away with many complexities and inconsistencies stemming from the current national implementing laws;
- they will strengthen the rights of individuals;
- they will make controllers more accountable for how they handle personal information;
- the role and powers of national supervisory authorities will be effectively reinforced at national level, but also at EU level through the European Data Protection Board (EDPB).

The EDPS expressed concerns, among other things on:

- the potential for restricting basic principles and rights;
- the possible derogation for transferring data to third countries;
- the excessive powers granted to the Commission in the mechanism designed to ensure consistency among supervisory authorities;
- the new ground for exceptions to the purpose limitation principle.

- the lack of a general duty for law enforcement authorities to demonstrate compliance with data protection requirements;

- the weak conditions for transfers to third countries;

- the unduly limited powers of supervisory authorities.

Throughout the year, the EDPS delivered various speeches elaborating our position on the reform package and took part in topical discussions. We have remained available to the EU legislator for further advice or explanation of our position. In addition, through our participation in the Article 29 Working Party, we gave input on several, more specific issues.

We also made efforts to foster further discussion. In September and November, in close cooperation with the Europäische Rechtsakademie (ERA), the EDPS organised two seminars dedicated to the proposals. The seminars brought together many experts from national administrations, data protection authorities, EU institutions, academia, third countries and the private sector. We also launched a webpage dedicated to the reform process, containing all relevant documentation, which is accessible via a link on our website.

The two proposals have been discussed extensively in the European Parliament and the Council and have attracted the attention of many public and private stakeholders. The lobbying surrounding the legislative process has been exceptional.

The LIBE Committee of the Parliament was nominated to lead the reform package. Two rapporteurs were appointed, one for the Regulation and one for the Directive and they worked together closely. Updates on the progress were given via several working documents which highlighted the points of departure and the main elements for further discussion. The annual Joint Parliamentary Committee Meeting in October was dedicated to the two proposals. The two draft reports were sent for translation before the end of 2012 and were publicly announced on 9 January 2013. The intention is to have a plenary vote in the second half of 2013. Draft reports of several other committees were also published around the end of 2012.

In the Council, the pace was slower. In a series of long, two-day meetings of the DAPIX working party, led by the Danish and the Cypriot presidencies, the Council worked through the proposals on an article-by-article basis. The Regulation was paid the most attention in these meetings since the proposed Directive has generally elicited less enthusiasm.

In parallel, the Council discussed several key themes, such as a possible division in the regulation between the public and the private sector, the lowering of the administrative burden for controllers and the broadening of powers for the Commission to adopt delegated and implementing acts. The Council, under the Irish Presidency, announced it would work at a quicker pace in 2013 and envisaged finalising the first reading in early 2013.

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

In 2012, we adopted a set of three formal comments and three opinions relating to the AFSJ and international cooperation.

3.4.1. EUROSUR

On 8 February 2012, we issued comments on a proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR). The aim of the proposal is better coordination between border control authorities, as well as border surveillance. To this end, Member States are to create national 'situation centres', whose assessments will then feed into a 'European situational picture' generated by FRONTEX.

Although the processing of personal information is not the aim of the proposal, such processing may occur under certain circumstances. We therefore recommended explicitly and exhaustively enumerating the conditions under which personal information may be processed in EUROSUR and to clarify the provisions on the exchanges of information with third countries.

3.4.2. Freezing and confiscation of proceeds of crime in the European Union

On 18 June 2012, we sent a letter to the Commission on the proposal for a directive on the freezing and confiscation of proceeds of crime in the EU.

Although the proposal does not directly involve the processing of personal information, the EDPS drew attention to aspects related to the impact some provisions may have on data protection when being implemented at national level.

3.4.3. European Cybercrime Centre

On 29 June 2012, we adopted an opinion on the Commission communication to establish a European Cybercrime Centre (EC3). We recommended that EC3's position and authority in relation to Europol's current legal framework and mandate be clarified. We also cautioned against the data protection risks inherent in the envisaged direct communication between EC3 and the private sector and the risks associated with international data transfers.

3.4.4. SIS II Migration

On 9 July 2012, we adopted an opinion on the Commission proposal for a Council regulation on migration from the Schengen Information System (SIS) to the second generation Schengen Information System (SIS II) (recast). When it is operational, SIS II will have enhanced functionalities, such as the potential to use biometrics, new types of alerts, the potential to link different alerts (such as alerts on a person and a vehicle) and a facility for direct queries within the system.

We welcomed the clarification in the proposal about the point during migration at which the SIS II Regulation will enter into force. However, we also highlighted the elements that could represent major risk and should be addressed to ensure that the migration will work as planned.

We recommended in particular: better definition of the scope of the migration within the proposal as it should be absolutely clear which data categories migrate; whether the migration involves any transformation of the data and if so, which ones; migration risks and the actions to mitigate such risks should be analysed; a specific obligation for data logging of the data processing activities of the migration should be provided for; the testing obligations should be strengthened; specific security measures in view of the risks of the migration should be introduced.

3.4.5. Human trafficking

On 10 July 2012, we issued our comments on the Commission communication for an EU strategy towards the eradication of trafficking in human beings (THB) for 2012-2016. We welcomed the strategy and its focus on the protection of fundamental rights but stressed that THB is an area that requires significant processing of data, in many cases involving personal information, consequently creating the risk of intrusion into privacy.

We emphasised that data protection is a precondition to mutual trust between victims and the authorities dealing with THB and also between authorities. We highlighted through practical and feasible suggestions, how data protection can contribute to a more effective and efficient cooperation between all the stakeholders.

3.4.6. EURODAC Regulation

On 5 September 2012, we adopted an opinion on the amended Commission proposal for a Regulation of the European Parliament and of the Council on the establishment of EURODAC for the comparison of fingerprints of asylum seekers. A significant addition to this amended proposal is the access to EURODAC data by law enforcement authorities.

Although the availability of a database with fingerprints could be a useful additional tool in combating crime, we considered that access to EURODAC for law enforcement purposes is a serious intrusion into the rights of a vulnerable group of people and we asked whether such access is truly necessary and proportionate.

However, should the necessity and proportionality of law enforcement access to EURODAC data be sufficiently demonstrated by solid evidence and reliable statistics, we still consider that more effective safeguards would need to be provided for in the proposal, such as a clear indication that the perpetrator has applied for asylum, truly independent verification and that the same conditions of access for Europol apply as for Member States.

3.4.7. CRIM Committee of the European Parliament

Set up in 2012 by the European Parliament, the purpose of the special Committee on Organised Crime, Corruption and Money Laundering (CRIM) is to analyse and evaluate the extent of these activities and their impact on the EU as well as the current implementation of EU legislation in this regard.

At the end of its mandate on 1 April 2013, the Committee must present its policy recommendations for measures and initiatives to be taken in these areas and in related security policies. These issues have considerable data protection implications, so we were pleased to receive a standing invitation for the meetings of the CRIM Committee. We have been following the work of the Committee and made contributions where relevant.

3.5. Internal Market including financial data

In 2012, we adopted a series of opinions dealing with internal market measures, including some focussing on financial markets.

3.5.1. Administrative Cooperation in the field of Excise Duties

On 27 January 2012, we adopted an opinion on the Commission proposal for a regulation of the Council concerning administrative cooperation in the field of excise duties. The proposal most notably aims to revise the provisions regarding automatic and requested information exchanges between Member States.

While closer cooperation between tax authorities could be useful to combat excise fraud, we consider that stronger safeguards regarding the processing and exchange of information are required.

3.5.2. Review of the professional qualifications directive

On 8 March 2012, we adopted an opinion on the Commission proposal to modernise and amend the existing text of the Professional Qualifications Directive. The two key aspects of the proposal are the introduction of an alert system and the introduction of a voluntary European professional card. The processing of personal information is to take place via the Internal Market Information System (IMI). We insisted that the proposed alert system should remain proportionate and called for further data protection safeguards. Taking into account proportionality and the balancing of rights and interests, including the presumption of innocence, we recommended, among other things, that the proposal should: specify that alerts can only be sent after a decision has been made by a competent authority or a court in a Member State prohibiting an individual to pursue his or her professional activities on its territory; specify that the content of the alert must not contain information regarding the circumstances and reasons for the prohibition; clarify and limit to the absolute minimum the period for which alerts are retained; ensure that the recipient authority keeps any alert information it receives confidential and does not further distribute or publish it, unless the information was made public in accordance with the law of the Member State sending it.

3.5.3. Reform proposals for financial markets

Several proposals in the financial area have raised the same data protection concerns, illustrating that a concerted effort needs to be made to address and incorporate data protection safeguards in financial proposals.

On 10 February 2012, we published a package of four opinions on Commission proposals for the reform of the financial markets legislation in the EU. The four proposals all concern the monitoring of financial data, which has a significant impact on the fundamental right to the protection of personal information. The opinions concerned the revision of banking legislation, the market abuse directive and regulation (MAD/MAR), the regulation and the directive on markets in financial instruments (MIFID/MIFIR) and the revision of the credit rating agencies regulation (CRA).

All these opinions raised similar data protection concerns. We, therefore, made the following overall recommendations: the inclusion of substantive provisions emphasising the applicability of existing data protection legislation; the addition of specific safeguards to the provisions for the transfer of data to third countries; the limiting of access to private premises; limit recording of telephone and data traffic to those instances where serious violations of the proposed legislation have been identified; clearly specifying the categories of telephone and data traffic records which need to be retained by financial institutions and/or provided to supervisory authorities; the assessment of necessity and proportionality of the proposed provisions on the publications of sanctions, supported by adequate safeguards; ensuring that the identity of whistleblowers

is protected; guaranteeing the right of the accused person to defence and to be heard, as well as the right to seek effective judicial remedy against any decision or measure concerning him/her.

3.5.4. Statutory audits

On 13 April 2012, we published an opinion on two Commission proposals regarding the statutory audit of annual accounts and consolidated accounts. The proposals raised data protection concerns in a number of areas including exchanges of information, record keeping, the publication of sanctions and the reporting of breaches.

3.5.5. European venture capital funds & social entrepreneurship funds

On 14 June 2012, we issued an opinion on the proposals for a regulation on European venture capital funds and for a regulation on European social entrepreneurship funds. Our main concern was that the proposed regulations are too general with regard to data protection issues. In some instances, it was unclear whether the processing of personal information will take place under some provisions of the proposed regulations, for example, exchanges of information, investigatory powers of the competent authorities and establishment of databases by the European Securities and Markets Authority (ESMA).

3.5.6. Improving securities settlement in the European Union

On 9 July 2012, we published an opinion on a Commission proposal on securities settlement in the EU and central securities depositories. It raised the issue of the investigative powers of relevant authorities and the exchange or transfer of information, requiring that specific safeguards be put in place.

3.5.7. Posting of workers in the framework of the provision of services

On 19 July 2012, we issued an opinion on the Commission proposal for a Directive of the European Parliament and of the Council on the enforcement of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services and on the Commission proposal for a Council regulation on the exercise of the right to take collective action within the context of the freedom of establishment and the freedom to provide services.

We welcomed the efforts made in the proposal to address data protection concerns and that the use of an existing information system, the Internal Market Information System (IMI), is proposed for administrative cooperation. On a practical level, the IMI already offers a number of data protection safeguards. Nevertheless, some concerns remain, relating mainly to bilateral exchanges, access to the registries and to the 'alert system'. We recommended further clarification and safeguards to address these concerns.

3.5.8. Insurance mediation, UCITS and key information documents for investment products

On 23 November 2012, we published an opinion on three Commission proposals regarding key information documents for packaged retail investment products, insurance mediation and protection for those who buy investment funds. Our main data protection concerns related to the need for clarification on the investigatory powers of the competent authorities, the establishment of a database by the European Insurance and Occupational Pensions Authority (EIOPA), the publication of administrative sanctions, including the identity of those responsible, and the reporting of breaches (so called whistle-blowing schemes).

3.6. Digital Agenda and technology

In 2012, the Commission dedicated significant efforts to furthering the implementation of the Digital Agenda and the EU 2020 Programme. Several of these initiatives had significant data protection relevance and were therefore closely followed by us.

Apart from the initiatives mentioned below, we also provided advice on additional proposals included in the Digital Agenda action plan, namely the legislative framework on collective management of copyright and related rights and multi-territorial licensing, the proposal for an EU-wide online dispute resolution system[11], the communication on a European Consumer Agenda[12] and the communication on a European Cybercrime Centre[13].

3.6.1. Cloud Computing

On 16 November 2012, we adopted an opinion on the Commission communication on *Unleashing the*

[11] See section 3.7.1.

[12] See section 3.7.3.

[13] See section 3.4.3.

potential of Cloud Computing in Europe to highlight the data protection challenges inherent in cloud computing. Allocating responsibility and accountability, and access to data "in the cloud", remain at the core of most of those problems. We therefore stressed the importance of establishing clear legal bases for these and other data protection principles to avoid ambiguity in their applicability and execution in practice.

Our opinion reacted not only to the communication but also highlighted the data protection challenges created by cloud computing and how the proposed data protection Regulation will tackle them when the reformed rules come into effect.

In our opinion on Cloud Computing, we highlighted the need for cloud service providers to take responsibility and be fully accountable for the services they offer so that together with cloud customers, they are able to fulfil their data protection obligations.

We also highlighted that the proposed data protection Regulation provides clear rules that, once adopted, would help guard against data protection responsibilities evaporating in the cloud. We also warned that the complexity of cloud computing technology does not justify any lowering of data protection standards.

Amongst our recommendations, we advised the responsible policymakers to:

- develop standard commercial terms and conditions that respect data protection requirements for commercial contracts, public procurement and international data transfers;
- clarify and provide further guidance on how to ensure the effectiveness of data protection measures in practice and the use of binding corporate rules;
- help develop best practices on issues such as controller/processor responsibility, retention of data in the cloud environment, data portability and the exercise of data subjects' rights;
- develop standards and certification schemes that fully incorporate data protection criteria and legally define the notion of transfer and the criteria under which access to data in the cloud by law enforcement bodies outside the EEA countries could be allowed.

3.6.2. Open Data Package

On 18 April 2012, we adopted an opinion on the open data package in which we highlighted the need for specific data protection safeguards whenever public sector information (PSI) contains personal information. We recommended that public sector bodies take a proactive approach when making personal information available for re-use and that a data protection assessment be carried out by the public sector body concerned before any PSI containing personal information is made available.

The proposal should include a data protection clause within the terms of the licence to re-use PSI. Where appropriate, the data should also be fully or partially anonymised, license conditions should specifically prohibit re-identification of individuals and the re-use of personal information for purposes that may impact data subjects.

In addition, the Commission should develop further guidance on anonymisation and licensing and consult the Article 29 Data Protection Working Party, an advisory body comprising data protection authorities from EU Member States and the EDPS.

3.6.3. Smart meters

On 8 June 2012, we adopted an opinion on the Commission recommendation on preparations for the roll-out of smart metering systems.

In our opinion we highlighted that while the Europe-wide rollout of smart metering systems may bring significant benefits, it will also enable massive collection of personal information which can track what members of a household do within the privacy of their own homes. We, therefore, warned that consumer profiling would track much more than energy consumption if not properly safeguarded.

In light of these risks, we called on the Commission to assess whether further legislative action is necessary at EU level. Furthermore, we provided pragmatic recommendations for such legislative action, suggesting that some of these can already be implemented via an amendment to the energy efficiency Directive, which was discussed in the Council and the Parliament at the time. This should at least include a mandatory requirement for controllers to conduct a data protection impact assessment and an obligation to notify personal data breaches.

Pending, or complementing, further legislative action, we recommended that the data protection impact assessment template (DPIA Template) be prepared by the Commission's Smart Grid Task Force and provide more guidance on: the legal basis of the processing and the choices available to data subjects (including frequency of meter readings); the use of privacy-enhancing technologies (PETs) and other techniques available for data minimisation; retention periods and how to provide direct access to consumers to their energy usage data, as well as recommendations to disclose individual profiles to consumers and the logic of any algorithms used for data mining and information on remote on/off functionality.

3.6.4. Electronic Trust Services Regulation

On 27 September 2012, we adopted an opinion on the Commission proposal for a regulation on trust and confidence in electronic transactions in the internal market, which will replace the current legal framework on e-signatures (set forth in Directive 1999/93/EC). The aim of the proposal is to enhance trust in pan-European electronic transactions and to ensure cross-border legal recognition of electronic identification, authentication, signature and related trust services.

We emphasised that compliance with data protection law is required for all data processing activities taking place under the proposal, in particular by: providing users of eTrust services with appropriate information on the processing of their personal data; specifying the types of personal information processed for cross-border identification; promoting the use of *privacy by design* techniques in electronic services that allow the disclosure of no or less personal information (e.g. pseudonymisation); defining a common set of security requirements in relation to trust services and identification schemes; ensuring that the data breach obligations introduced in the proposal are consistent with those foreseen in other data protection legislation (ePrivacy directive and the proposed data protection regulation).

3.6.5. Better Internet for Children

On 17 July 2012, we issued an opinion on the European strategy for a *Better Internet for Children* put forward by the Commission. The strategy lists a number of actions for industry, Member States and the Commission. They include the fostering of parental controls, privacy settings, age ratings, reporting tools, hotlines and cooperation between industry, hotlines and law enforcement bodies.

We welcomed the recognition of data protection as a key element and illustrated specific means by which the protection and safety of children online can be enhanced from a data protection perspective. In particular, we recommended: inclusion of references to data protection risks and prevention tools in awareness raising campaigns; implementing more protective default privacy settings for children including changing default settings; deployment of appropriate tools for age verification which are not intrusive from a data protection perspective; avoid specific targeting of minors for direct marketing and for behavioural advertising. We called on the Commission to help promote privacy friendly, self regulatory measures and to look into the possibility of further legislating at EU level.

We also raised concerns about the initiatives for the fight against sexual abuse and sexual exploitation of children on the internet, including: an appropriate legal basis for reporting tools and with a clear definition of the type of illegal activity that can be reported; better defining and harmonising the procedures for reporting through hotlines, for instance, through a European code of practice defining common reporting procedures and a reporting template which embeds data protection safeguards; clearer and more defined modalities for cooperation between industry and law enforcement.

The right balance should be struck between the legitimate objective to fight against illegal content and the nature of the means used. Some tasks, such as the surveillance of telecommunications networks, should remain primarily within the competence of law enforcement.

3.6.6. Network and Information Security in the EU

In our comments of 10 October 2012 on a strategy for network and information security (NIS) in the EU, we emphasised the importance of considering data protection when devising such a strategy. We focused on the issues of clear definitions for cybersecurity threats and the reporting thereof, the conditions and safeguards for the exchange of information between private actors and public bodies and stressed the opportunity presenting itself in this context to implement principles such as *privacy by design*.

3.6.7. Open Internet and Net Neutrality

On 15 October 2012, in response to the Commission's public consultation, we pointed out that internet traffic management practices raise data protection concerns, as highlighted in the details of our opinion on net neutrality (7 October 2011).

Among other things, many data protection principles – such as the principles of purpose limitation, proportionality and accountability – should guide the deployment of alternative, less privacy intrusive methods. We also suggested ways in which internet service providers could improve transparency of their internet traffic management practices for end users, in particular by providing information about more intrusive forms of processing and on how end users may withdraw consent in cases where it is relied upon as a legal basis for the processing.

3.7. Public health and consumer affairs

In 2012, we adopted a set of formal comments and three opinions in the field of public health and consumer affairs on several Commission proposals.

3.7.1. Cross-border Alternative Dispute Resolution for consumer disputes and a Regulation creating an Online Dispute Resolution platform

On 12 January 2012, we adopted an opinion on the proposals for a directive on cross-border alternative dispute resolution (ADR) for consumer disputes and a regulation creating an online dispute resolution (ODR) platform.

Although data protection principles had already been taken into account in the proposals, we recommended that the responsibilities of data controllers be specified, data subjects be informed accordingly and the limitation of access rights be clarified.

3.7.2. Early Warning Response System and cross-border threats to health

On 28 March 2012, we adopted an opinion on the Commission proposal to expand the existing early warning response system (EWRS) to include new cross-border threats to health, such as hazards of biological, chemical, or environmental origin.

We recommended that the rules on contact tracing be clarified as well as the relationship between the EWRS and the proposed *ad hoc surveillance networks*. We also recommended that the requirements on data security and confidentiality be specified.

3.7.3. European Consumer Agenda

On 16 July 2012, we published comments on the European consumer agenda – *boosting confidence and growth* – which proposed the creation of synergies between initiatives in the fields of consumer affairs and those aimed at improving the protection of personal information, particularly in the digital environment.

Awareness raising campaigns, training programmes and codes of conduct such as those proposed by the European consumer agenda can be even more powerful if they incorporate privacy and data protection elements.

3.7.4. Clinical Trials

On 19 December 2012, we adopted an opinion on the Commission proposal on clinical trials on medicinal products for human use. We welcomed the attention paid specifically to data protection in the proposed regulation, but identified room for improvement.

We recommended that the proposed regulation should explicitly refer to the processing of personal information concerning health; clarify whether personal information concerning health is to be processed in the EU databases for clinical trials, and if so, for what purpose; refer to the right of the data

subjects to block their personal information and introduce a maximum retention period for the storage of personal information.

3.8. Publication of personal information

Achieving a balance between transparency and data protection is a re-occurring theme in our work. In 2012, we adopted several opinions in which the publication of personal information was a core issue.

This was first the case in the package of opinions we published on 10 February, on different proposals for the financial market[14]. These proposals included the 'naming and shaming' of companies and individuals. Similar issues arose in the opinions on improving securities settlement in the European Union[15] (9 July) and on insurance mediation, UCITS and key information documents for investment products[16] (23 November).

In all these opinions we emphasised the need to balance the principle of transparency, the right to privacy and data protection and the need for specific safeguards. We emphasised that the role of privacy and data protection is not to prevent public access to information whenever personal information is involved or to unduly limit transparency. Privacy and data protection should ensure that personal information is published only when justified and in a manner which takes into account the different interests involved.

The scope of public disclosure of personal information should be analysed proactively at the earliest stage, informing the persons involved accordingly to allow them to exercise their rights.

On 18 April 2012, we adopted an opinion on the open data package.[17] As this proposal included measures to facilitate a wider re-use of public sector information (PSI), we asked for more details about the possible situations in which personal information may be made available for re-use and under which conditions.

We analysed the different proposals in light of the Court of Justice rulings in *Bavarian Lager* (C-28/08P) and *Schecke* (Case C-92/09 and C-93/09). The amendment to the proposal for financing, manage-

[14] See section 3.5.3.

[15] See section 3.5.6.

[16] See section 3.5.8.

[17] See section 3.6.2.

ment and monitoring of the Common Agricultural Policy (CAP) on which we adopted an opinion on 9 October 2012, was actually a follow-up to the *Schecke* ruling, in which EU legislation on the disclosure of personal information of farmers receiving money from EU funds was annulled because less privacy intrusive measures had not been considered.

In several proposals, the Commission had clearly sought to strike a balance between transparency and data protection in the proposed legislation. Our main comments related to the lack of a clear definition of the purpose of the disclosure.

Furthermore, there was no indication that the different methods, modalities and levels of detail of making personal information publicly available in order to find the least intrusive measure had been considered carefully. We often had to highlight the sensitive nature of the information involved (e.g. personal data revealing political opinions or relating to offences) which need to be taken into account when assessing and justifying their publication and when foreseeing suitable safeguards.

This also applies to the proposal for a statute and funding of European political parties and European political foundations on which we adopted an opinion on 13 December 2012. In our recommendations, we addressed a number of relevant details relating to the publication of data on members, donors and contributors of those bodies.

3.9. Other issues

In 2012, we also issued opinions on subjects in which data protection was not the central, but rather a related issue: a proposal for a Regulation establishing the European voluntary humanitarian aid corps, and a Commission proposal for a Council Regulation regarding the deposit of the historical archives of the institutions at the European university institute in Florence.

3.10. EDPS policy on access to documents

As an EU institution, the EDPS is subject to the public access to documents Regulation of 2001. The number of public access requests for documents held by the EDPS has increased in comparison to previous years. In 2012, we received **10** requests for access to documents and were consulted **twice** by other institutions concerning requests submitted to them. Access to documents or information was granted in all 12 of these cases.

In order to consolidate our existing practice and to ensure a consistent application of the rules, we

adopted a case manual to guide EDPS staff on dealing with public access requests. An assistant has been specifically assigned the task to ensure the proper implementation of this case manual.

To highlight the importance that we place on this issue, we are planning a section on our website dedicated to our transparency policy. It will outline the policy and contain an easy-to-use tool to request access to documents. The dedicated webpage is scheduled to go online in 2013.

3.11. Court matters

No EDPS decisions were challenged before the Court of Justice of the EU in 2012 and we did not instigate any proceedings against other EU institutions or bodies. The court ruled on two cases in which we acted as intervening party. In addition, we requested leave to intervene in two other cases which are still pending.

The first ruling dealt with the alleged lack of independence of the Austrian data protection authority, the Datenschutzkommisson (DSK). In *Commission v. Austria* (Case C-614/10), we intervened on behalf of the Commission.

In its ruling of 16 October 2012, the Court concluded that the Austrian DSK did not fulfil the requirements of independence as outlined in the data protection Directive. In particular, the Court considered that the DSK's functional independence from the Government as provided for under Austrian law was not sufficient and that its close ties with the Federal Chancellery prevented the DSK from being above all suspicion of partiality.

This was the second court case centred on the independence of data protection authorities, following *Commission v. Germany* (Case C-518/07), in which we had also intervened on behalf of the Commission. We strongly welcomed the Court's ruling of 9 March 2009, which was largely in line with our argument in our intervention and the court hearing in April.

Our reaction to the ruling in *Commission v. Austria* was that the Court had once again stressed the legal obligation of complete independence in a data protection authority. This ruling supports the importance of data protection as a fundamental right and the need for impartiality in order to safeguard it effectively in national law. The Court's decision is also important for the review of the data protection framework, which must strengthen the role of the data protection authorities.

The second case in which we were involved was *Egan and Hackett v. European Parliament* (Case T-190/10). This was the last of three cases in which the General Court had to rule on the relationship between the public access to documents Regulation and the data protection Regulation, after the leading ruling in *Bavarian Lager v. Commission* of 29 June 2010 (Case C-28/08 P). We had also acted as an intervening party in the other two cases, *Valero Jordana v. Commission* (Case T-161/04) and *Dennekamp v. European Parliament* (Case T-82/09), which were decided in 2011.

The two applicants in this latest case requested public access to two documents relating to the applications for parliamentary assistance allowance of two MEPs in which names of assistants were mentioned. The Parliament refused to grant access on the grounds that the names constituted personal information, the disclosure of which would infringe the privacy interests of the individuals concerned.

The EDPS intervened on behalf of the applicant arguing that the Parliament had failed to conduct a concrete and individual examination under the access to documents regulation and had failed to consider possible access under the data protection regulation. In its ruling of 28 March 2012, the Court annulled the refusal, as the Parliament had failed to show to what extent the disclosure of documents containing the names of former MEP assistants would specifically and effectively undermine their right to privacy.

The first case, still pending at the time of writing, is another infringement action concerning the independence of data protection authorities, this time against Hungary (Case C-288/12). The EDPS has requested leave to intervene.

The second pending case is *ZZ v. EIB,* before the Civil Service Tribunal (Case F-103/11). During an internal harassment investigation conducted by the EIB, the full complaint on the alleged harassment, including the associated documents (which included medical declarations) was sent to those accused of the harassment. The applicant claimed that this was contrary to the data protection Regulation. The EDPS intervened in support of the applicant in as far as the claim was based on an alleged breach of these data protection rules.

In 2012, the EDPS closely followed several other cases without intervening: first, in the Spanish Google case (Case C-313/12) questions were submitted to the Court of Justice on the applicability of Spanish law implementing the European data protection directive on Google activities, which on the whole are physically performed outside the EU.

Two other cases related to the validity of the European Data Retention Directive. This Directive requires Member States to oblige telecom providers to store telephone data (except the content of conversations) of their customers for a period between 6 and 12 months. In Germany, after the implementing measure was annulled by the Constitutional Court, no new law was enacted. The European Commission took Germany to court for infringing EU law by failing to implement the Directive (Case C-329/12). Germany justified its inaction by arguing that the Directive was contrary to the Charter of Fundamental Rights. The same question on the conformity of the Data Retention Directive with fundamental rights was raised in a preliminary ruling requested by an Irish Court (Case C-293/12). The Court of Justice did not rule on any of these three cases in 2012.

3.12. Priorities in 2013

In January 2013, the EDPS will publish the seventh public inventory as an advisor on proposals for EU legislation, setting our priorities in the field of consultation for the year ahead. We face the challenge of fulfilling our increasing role in the legislative procedure whilst guaranteeing high-quality and well-appreciated contributions to it, to be delivered with limited resources.

There are several notable trends in recent years which merit attention from a data protection perspective:

1. The need to take account of privacy and data protection implications of legislative proposals is becoming essential in all areas of EU policy. It is increasingly apparent that the fundamental right to data protection cannot be regulated only in data protection law but that many different policy areas have to take data protection into account.

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 AFSJ and in relation to the revision of the legislative framework concerning financial supervision.

3. In this context, the increasing importance of internet monitoring by public authorities as well as by private parties, must be considered in relation to irregularities on the internet, from combating child pornography to cybercrime to intellectual property rights.

4. EU legislation increasingly facilitates significant exchanges of information between national authorities, quite often involving EU-bodies and large-scale databases (with or without a central unit) of increasing size and processing power. This needs careful consideration by policy makers and actors in the legislative process when setting out data protection obligations, due to the consequences these exchanges can have on the privacy of citizens, for instance, by facilitating the monitoring of citizens.

5. Recent years have been characterised by impressive technological developments, mainly due to the widespread use of the internet and geo-location technologies. Such developments have a significant impact on a citizen's right to privacy and data protection.

Such policy and technological developments highlight that data protection and privacy have become truly horizontal issues. This means that there will be more demand for our advice on proposed legislative measures at a time of limited resources.

Our Strategy for 2013-2014 therefore laid down as a general principle that we will focus our attention and efforts on areas of policy that present the highest impact on privacy and that we will act selectively and proportionately.

Subject to these considerations, we are committed to devoting substantial resources in 2013 to the analysis of proposals of strategic importance.

Additionally, we have identified a number of less obvious initiatives of lesser strategic importance which may become relevant for data protection. The fact that the latter are included in our inventory implies that they will be monitored regularly, but does not mean that we will always issue an opinion or formal comments on them.

Our main priorities, as identified in the 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. Technological developments and the Digital Agenda, IP rights and the Internet
   - Internet monitoring (e.g. the fight against child pornography and enforcement of IP rights)
   - Cyber-security
   - Cloud computing

c. Further developing the Area of Freedom, Security and Justice
   - Eurojust Reform
   - Europol Reform
   - Cybercrime
   - Smart Borders package
   - Negotiations on agreements with third countries on data protection

d. Financial sector
   - Regulation and supervision of financial markets and actors
   - Banking supervision
   - Anti money laundering

e. eHealth
   - Proposals on clinical trials and medical devices.
   - eHealth action plan

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 (the Working Party) is an independent advisory body set up under Article 29 of Directive 95/46/EC. 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.

The Article 29 Working Party is composed of representatives of the national data protection authorities, the EDPS and the Commission (the latter also provides the secretariat for the Working Party). It plays a central role in ensuring the consistent application of Directive 95/46/EC.

In 2012, we continued to actively contribute to the activities of the 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.

We have also been acting as a rapporteur or co-rapporteur for the opinion on purpose limitation and compatible use (Key Provisions subgroup); the opinion on smart grid data protection impact assessment template (Technology subgroup); and the opinion on open data (eGovernment subgroup). All three opinions are expected to be adopted in early 2013.

In addition, we made significant contributions to the opinions adopted in 2012, particularly: data protection reform discussions (two opinions)[18], cloud computing[19], cookie consent exemption[20] and developments in biometric technologies.[21]

Moreover, we contributed to other activities of the Working Party where it stated its position in the form of letters. A prominent example is the letter on the changes in Google's privacy policy.

[18] Opinion 08/2012 providing further input on the data protection reform discussions – WP 199, 05.10.2012 ; opinion 01/2012 on the data protection reform proposals – WP 191, 23.03.2012

[19] Opinion 05/2012 on Cloud Computing – WP 196, 01.07.2012

[20] Opinion 04/2012 on Cookie Consent Exemption – WP 194, 07.06.2012

[21] Opinion 03/2012 on developments in biometric technologies – WP 193, 27.04.2012

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

Direct cooperation with national authorities is an element of growing importance in the development of large-scale international systems, such as EURODAC, which require a coordinated approach to supervision (see Section 4.2.).

4.2. Coordinated supervision

4.2.1. EURODAC

Effective supervision of EURODAC relies on close cooperation between the national data protection authorities and the EDPS.

EURODAC is a large-scale IT system devoted to storing fingerprints of asylum seekers and persons apprehended irregularly crossing the external borders of the EU and several associated countries.[22]

The EURODAC Supervision Coordination Group is composed of representatives of the national data protection authorities and the EDPS. We also provide the secretariat for the Group and as such, we organised two meetings in Brussels in 2012, one in June and one in November. The Group based its 2012 activities on the 2010-2012 work programme and several activities were undertaken in 2012:

[22] Iceland, Norway, Switzerland and Liechtenstein.

A methodology for national inspections

One of the group's most significant achievements of the year was the standardised inspection plan for EURODAC National Access Points (NAPs), adopted at the meeting in November. The purpose of the questionnaire is to assist, without being prescriptive, national inspections. The questionnaire covers the formal and informal procedures in place to ensure the secure and authorised collection, storage, handling, transmission and any other processing of EURODAC information within, between, to and from the NAPs and the Central Unit.

Unreadable fingerprints exercise

At both 2012 meetings of the EURODAC group, the ongoing preparations for the unreadable fingerprints exercise were discussed. It was generally agreed that both asylum seekers and asylum authorities would benefit from a unified practice within the EU. Work is ongoing, with an aim of adopting the final report by mid-2013.

The next meeting of the EURODAC group will be held in Spring 2013.

4.2.2. VIS

The Visa Information System (VIS) is a database of 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 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 became operational in North Africa in October 2011. Thereafter, VIS was implemented in two other regions, the Near East in May 2012 and the Gulf Region in October 2012.

In November 2012, we hosted the first meeting of the VIS Supervision Coordination Group. The Group, which comprises national DPAs and the EDPS, is tasked with overseeing the gradual roll-out of the system, to look into any issues such as those relating to the outsourcing by Member States of common tasks to external providers and to share national experiences.

The VIS Group discussed its first draft working programme and shared information on EDPS activities

and national inspections in different Member States. The next meeting will be held in Spring 2013.

4.2.3. CIS

The purpose of the Customs Information System (CIS) is to create an alert system within the framework of combating fraud so that any Member State can input information into the system and request another Member State to carry out sighting and reporting, discreet surveillance, specific checks or operational and strategic analysis.

The CIS stores information on commodities, means of transport, persons and companies and on goods and cash detained, seized or confiscated. The information can help to prevent, investigate and prosecute actions which are in breach of customs and agricultural Community rules (the former EU first pillar) or serious contraventions of national laws (the former EU third pillar). The latter is due to its legal basis 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 in which the data protection authorities, responsible for the supervision of CIS in accordance with Regulation (EC) No 766/2008[22]. The EDPS and national data protection authorities cooperate in line with their responsibilities in order to ensure the 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.

As the secretariat for the CIS Group, we organised two meetings in Brussels in 2012 (in June and December). In the June meeting, the group adopted in cooperation with the Customs JSA a joint opinion on the FIDE handbook and the activity report for the preceding two years. Following discussions on the state of play of the recast of Regulation (EC) 515/1997, two working documents were distributed to the group which are to be developed into full reports for the next meeting.

In the December meeting, the EDPS presented the key points of the follow-up of OLAF prior checks, which was followed by a presentation by the Commission (OLAF) on recent developments in the impact assessment of the amendment of Council Regulation 515/97 and technical developments of the CIS. The secretariat presented two draft reports which subject to pending replies and a few further clarifications, outlined potential group activities for 2013, namely to assess the appropriateness of access to CIS and FIDE and to investigate opportunities to increase awareness of data subjects rights.

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.

[23] 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.

On 3-4 May 2012, the **European Conference of Data Protection Commissioners** took place in Luxembourg. The conference focused on recent developments in the modernisation of the data protection framework of the EU, the Council of Europe and the OECD. The Conference recognised the current efforts seeking to guarantee enhanced rights for citizens and consumers and effective ways for exercising them, while taking into account technological changes and globalisation.

A great deal of attention was paid to the European data protection reform at the conference. The Data Protection Commissioners adopted a resolution welcoming many aspects of the Commission proposals aimed to strengthen the rights of individuals and consistency but noted that further improvements were needed, especially to bring the proposed directive regarding the area of police and justice in line with the core principles of the proposed general data protection regulation.

4.4. International conference

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

The 34th annual **Conference of Data Protection and Privacy Commissioners** took place in Uruguay on 25-26 October 2012 with more than 90 speakers representing 40 countries. The main focus of the conference on the general theme *Privacy and Technology in Balance* was the phenomenon of 'big data'. The list of distinguished speakers included Peter Hustinx, EDPS and Giovanni Buttarelli, Assistant EDPS, both of whom moderated different panels.

At the conference, two Resolutions – on cloud computing and on the future of privacy – were adopted. There was also an emphasis on the need for enhanced co-operation in order to ensure a high level of privacy, data protection and IT security to reduce the risks associated with the use of cloud computing services and to face common privacy challenges and future concerns more efficiently.

Following the discussions in Mexico City in 2011 on the increasing amount of personal information being collected and processed by both private and public sector entities from around the world (*big data*), the Uruguay Declaration on profiling was adopted. The Declaration highlights that general data protection and privacy principles, specifically the principle of purpose limitation, will remain the basis on which processing operations should be judged.

Many side events were organised before or in parallel to the conference, for instance, the Public Voice Conference with participation from civil society and a reception organised by the Council of Europe to celebrate the forthcoming accession of Uruguay as the first non-European member to Convention 108.

The 35th International Conference will take place in Warsaw in September 2013.

4.5. Third countries and international organisations

4.5.1. Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data

Opened for signature in 1981, Convention 108 of the Council of Europe contains a set of data protection safeguards for individuals in light of the increasing flow of information across borders in automated processes. The Convention laid the basis for Directive 95/46/EC, and is is now subject itself to a separate review process. In our function as an observer with the right to intervene, the EDPS attended two meetings of the Consultative Committee of Convention 108 in 2012, one in September and one in November. These meetings were particularly important for us to follow and influence the ongoing modernisation of the Convention.

In the September meeting, the Bureau of the Consultative Committee discussed the proposed changes of the Convention text. We proposed several ways to strengthen data protection such as harmonising the proposed text to ensure consistency within the Convention, retaining the requirement for *explicit consent* and clarifying the difference between *processing* and *filing system*. Following the meeting, an amended version of the text was circulated for written comments.

The new provisional draft of the Convention, which took many of our recommendations into account, was adopted in the November meeting. The meeting was concluded with the agreement that a draft of the updated Convention would be sent to the Council of Ministers in early 2013.

4.5.2. International Workshop on data protection in international organisations

On 8-9 November 2012 in Brussels, the World Customs Organisation (WCO) organised the 4th International Workshop on data protection in international organisations with our support. The workshop provided a forum to discuss data protection within international organisations. It assembled professionals from EU institutions and bodies and international organisations to discuss and share best practice.

Several panels moderated by representatives of both the EDPS and the WCO took place over the two day event. These were an opportunity to update participants on recent developments relevant for international organisations, including those on data protection (Council of Europe and OECD) as well as the European data protection reform package, compliance and transfers of data to third parties, the processing of staff data, security breach and notification and cloud computing. The workshop was once again successful in facilitating exchange between the participants, contributing to even greater cooperation and sharing of experiences between DPOs of EU institutions and bodies and relevant staff of other international organisations.

5 MONITORING OF TECHNOLOGY

5.1. Technological development and data protection

Developments in technology have often created challenges for privacy. New information and communication technologies have, in turn, also triggered legislative and regulatory responses. The rapid advancement of the state of the art in IT impacts a broad spectrum of society with the associated risks of processing personal information and increases the significance of privacy and data protection.

In order to make meaningful contributions in this area, data protection authorities, including the EDPS, have to provide analysis that takes into account the current technological opportunities and threats. In response, during our strategic review process as outlined in chapter 1.2, we have adjusted our internal organisation structure and established an IT Policy sector to provide relevant expertise and insight and reinforce our capacity to monitor technological developments. This chapter is part of that function, demonstrating the forward-looking analysis of our IT experts of the various matters discussed.

By continuously assessing technological developments and their potential impact on data protection, the sector supports our supervision and enforcement as well as policy and cooperation tasks.

- 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 hosting of the future case management system.

5.2. Future technological developments

5.2.1. Data protection principles must work with new technologies

Since its infancy in the 1970s, the potential of automated data processing has been a driving force in society's efforts to protect the fundamental rights of individuals. Even in those days, when the power of mainframe computers was less than that of a smart phone today, the promoters of data protection were aware of the potential offered by technology to exercise control over individuals and to restrict personal freedoms.

Basic principles, such as transparency, purpose limitation, data minimisation and independent supervision laid the foundation for data protection and have developed along with societal, economic and technological changes. They were created with enormous foresight and they are still valid in today's world. Having overcome the technical limitations of the past we are faced with entirely new ways of processing, so it is all the more necessary to monitor and assess these technological developments to ensure their effectiveness in data protection. We are charged to perform such monitoring by the data protection Regulation that established the EDPS and to inform the public and the European legislator of the relevance of these developments.

5.2.2. Business developments

Big data will be a driver of developments in information and communication technology.

It is generally accepted that the developments classified under *big data* are a direct result of advances in information technology, which make the establishment of multi-petabyte data warehouses possible and the processing of huge amounts of information affordable. It is claimed that daily production of data has grown to 2.5 quintillion bytes of data[24], which means that almost all existing digital content (90%) has been produced in the past two years. The rate of production can only increase in the future.

While the quantities are impressive, the quality still needs to be defined: the notion of *big data* still lacks a clear and universal definition. Currently, *big data* is defined as mass quantities of data of multiple types, which are used for improving consumer experience – and eventually, increased returns in investment[25]. Future development will lead to more precise notions of *big data* and to the differentiation of the various categories and fields of application.

The current measures to implement *open data* policies, providing public sector data for exploitation in the private sector, is expected to become a focal point for *big data* initiatives. At the same time, the number of analytical applications managing diverse forms of data produced by individual use – such as text, video and audio – will increase considerably.

The clarification of *big data* will proceed in parallel with efforts to overcome the technical challenges that the processing of huge amounts of data is still posing. Both public and private sectors have an interest in producing *actionable information*[26], which could contribute to improved efficiency, productivity, decision making and general performance.

With better understanding of methods and tools for the analysis of *big data* and the differentiation of the fields of application, it will become clear that not all *big data* is necessarily *personal* data. Yet there is no doubt that the processing of *big data* will create challenges for the protection of personal information. One area where this can be observed is in the field of *social data*, which is produced by the active use of social networks.

Social networking services have matured and become relevant to all generations and professions.

While *social networking services* must continue to acquire new users to survive, if only to maintain and rejuvenate their population, it is likely that more *social data* will be produced per user. To

[24] <http://www-01.ibm.com/software/data/bigdata/>

[25] M. Schroeck, R. Shockley, J.t Smart, D. Romero-Morales and P. Tufan ' Analytics: The real-world use of big data. How innovative enterprises extract value from uncertain data' <http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03519usen/GBE03519USEN.PDF>

[26] See footnote 25

some extent this will be triggered by increased functionality and more intensive use of applications within social media services, on the social graphs of their users.

Increased activity will result in an increase in constant news feeds and usage time. More importantly, in order to monetise their efforts, social networking services endeavour to enrich their collections of personal information by partnering with external services. Social network users are already awarded access on the basis of their social profile credentials of various online services and platforms, such as content (music, video), games, special social services (dating, travelling) or shopping. With these connections, a social networking service can gather information about the transactions of its users in these connected services and can increase the commercial value of its data collection, for marketing and advertising for instance.

Furthermore, social media are likely to offer new and more targeted services both for businesses and consumers, based on increasingly sophisticated analysis and profiling. Social graphs, in other words, the data representation of the relationship between the individuals using a social networking service are likely to provide a greater insight into specific user groups (exploiting brand and celebrity preferences, such as fan pages and so on). Services based on these techniques are also offered to consumers and are able to run more exhaustive searches based on their personal profile so as to intensify relationships based on common interests.

Business interests in the commercial use of location data will subsequently lead to the development of advanced anonymisation techniques.

Communication devices increase their data collection capabilities beyond pure communications data. *Mobile location based services* will play a key role in the increased use of location data. As location data can be particularly privacy intrusive, the EU legislator has imposed strict limits on its use, for example, in the legislation on electronic communications and on the retention of communications data for law enforcement purposes.

Location related data from other sources, such as from RFID usage, or the *internet of things* more generally, has been the subject of political and scientific debate seeking to mitigate the privacy impact of these technologies. In exploring ways to generate higher revenues, businesses will be attracted to the huge amounts of location data produced by *geographic information* and *global positioning systems*, which are an integral part of most smart devices. Yet in order to benefit from the use of location based services, industry has to ensure that consumers are both reliant and aware of their data being collected and used.

One way to reduce the privacy impact of location data could be the application of anonymisation algorithms. The effectiveness of "location data anonymisation" to protect individual privacy is a much mooted, perhaps even controversial subject between computer scientists. There is strong evidence that removing all identifying attributes from the data is not effective. Additional techniques such as *blurring* (reducing accuracy of locations) and exclusion of certain areas (private sphere) from location tracking as well as limitation of the tracking periods are supporting options.

There is no doubt that these techniques will attract the attention of industry[27]. Experience gathered from current practices in some markets, such as China, Japan and South Korea, will be re-shaped to fit African, European and North American frameworks.

A demand for embedded privacy and security in smart devices is expected to increase.

Smart devices, such as smart phones, tablets and other connected services, are extending and reshaping our opportunities to interact. Collecting, communicating and processing data in real-time provides unprecedented added value services to users. These services range from contextual services linked to location data, proximity sensors and the automatic adaptation to consumer preferences, to mobile health services where medical information is processed and communicated to practitioners and health centres, to the use of smartcards via smart phones for payments, which is possible due to NFC[28] technology.

In this environment, users face data control and management challenges. Information is often col-

[27] For more information, see J. Wood, 'Preserving Location Privacy by Distinguishing between Public and Private Spaces' http://locationanonymization.com/PrivateSpaces.pdf

[28] Near Field Communication

lected by default and not in a transparent way. Large amounts of information are transferred to app owners and behavioural advertising operators without obtaining free and informed consent, offering inadequate information, if at all, on the manner and the reason for collection and further use of personal information. Mobile security is not yet mature enough to handle the critical nature of the information processed.

Secure, trustworthy and privacy-friendly mobile environments that also guarantee smooth user experiences will thus be of the utmost importance for steady uptake and safe and secure use of smart devices and related services. All actors in the value chain, including platform developers, app developers, app stores and carriers need to contribute to this development.

The use of smart meters grids will prove to be advantageous, once privacy and security concerns are eliminated.

Intelligent and rationalised production, distribution and use of energy, specifically electricity and gas, are crucial for a sustainable economy. Smart meters and smart grids are considered key enablers in guaranteeing the availability of power supply and offering customers (individuals as well as industry) opportunities in cost savings and environment-friendly behaviour. To this end, user-related information is collected: mainly consumption through periodic readings and possibly, other more fine-grained information in the future.

Industry, consumer associations and other stakeholders are working together with the Commission to co-ordinate actions for the roll-out of smart meter and smart grid systems. Standardisation efforts and other activities are being carried out to obtain interoperability, secure operation and user acceptance by showing the advantages and ensuring privacy and protection of customers' personal information.

With the roll-out of the smart grids, privacy and security risks will increase. The use of various communication networks and the shift of hacking activities towards critical infrastructures, industry and the *internet of things* increase cyber-security risks. The collection of consumer behaviour information could encourage energy operators to monetise personal information.

Customer privacy will need to be safeguarded by guaranteeing basic principles, such as data minimisation or avoidance, necessity and purpose limitation. *Privacy by design* and *best available techniques* (BAT) are privacy principles that need to be enforced – such as the use of anonymisation/pseudonymisation and aggregation techniques. Data

protection impact assessments (DPIAs) are tools for a risk-based assessment of privacy risks.

To increase the number of users, cloud service providers will need to ensure they meet data protection obligations.

Cloud computing is expected to fundamentally reshape the IT industry. Compared to the traditional IT service provisioning model, it can offer substantial benefits to individuals and organisations, such as lower costs, increased flexibility, faster implementation and payment for use rather than for capacity. Extreme growth is expected for the cloud services market.

So far, the development has not fully confirmed expectations. Many businesses fear that by moving to the cloud they will give up control of their information infrastructure, hence the lack of confidence in the service. Some cloud based solutions feature a high potential risk of vendor lock-in. Concerns about security are also perceived as a real problem. Technologies addressing these issues are still in their infancy and are tailored for specific cloud providers, or specific *software-as-a-service* solutions. Considerable efforts in development and standardisation are needed to establish widely accepted levels of security.

Cloud computing is a trend that clearly cannot be ignored by the European institutions. It will, therefore, be necessary to develop Guidelines for the use of cloud computing in public administrations. As outlined in our recent opinion on the subject, a major challenge is the fact that cloud customers typically have little influence over the terms and conditions of the service offered by cloud providers. Cloud customers need to ensure that they are able to fulfil their data protection obligations nonetheless.

5.2.3. Law enforcement and security

Innovative methods to gather evidence from the cloud environment will be developed.

As cloud computing becomes more widespread, it is likely to attract criminal applications, either as a resource in support of criminal activity, or as its target. Faced with this development, law enforcement authorities will need to find new ways of conducting investigations and of collecting and preserving evidence.

As an emerging discipline, cloud forensics is the application of science for the identification, collection, examination and analysis of data in the cloud, while preserving the integrity of the information and maintaining a strict chain of custody for the data. The cloud environment adds complexity, in that evidence can be gathered remotely, from virtual machines available on the network and on a large scale.

The process is complicated further because of the need to involve many cloud actors such as providers, consumers, brokers, carriers and auditors and because of the multi-tenancy and multi-jurisdictional legal position. In this context, it would be easy for actors in cloud forensics to lose sight of privacy considerations. It is clear that creative solutions must be developed to ensure that the privacy of data subjects sharing the cloud infrastructure is not compromised by forensic activity.

Data protection authorities will be faced with the same difficulties.

Automated Border Controls will improve border controls.

As numbers of travellers continue to rise, existing infrastructures at international border crossings will be under extreme pressure to deal with the increased throughput. To maintain the service in a cost effective way, new approaches and solutions are being developed. *Automated border controls* (ABC) aim to automate passenger checks at border crossing points using new technologies with the supervision of border guards. Using ABC, border guards will focus on those considered risky and allow the majority of passengers to use the automated system.

While there is strong support for the implementation of ABC, the timing and methods are yet to be determined. As to *when*, the main challenges are to ensure the interoperability between systems globally, to make travellers comfortable with the use of ABC, re-train border guards to balance security and facilitation. The *how* still needs to be defined, but it is evident that biometrics, which continues to raise data protection concerns, will play a key role in ABC. Currently, the most commonly used methods are fingerprint and facial recognition, however

other methods (iris scans, for instance) are likely to be introduced before too long.

Furthermore, as border control systems become increasingly automated, there will be demand for their integration with central databases (such as SIS, VIS, databases of known criminals and so on) which will also raise data protection concerns.

The use of portable body scanners will change police operations.

The use of body scanners in European airports began around 2007 and their use has spread throughout the world. In 2010, Dutch police were considering the implementation of this technology on their streets in a portable format, to check for concealed weapons at a distance thus avoiding individual body searches. In the United States, similar programs have begun and in early 2012, the New York police department (NYPD) began testing these devices mounted on their vehicles. At the beginning of 2013, the NYPD took delivery of these portable body scanners.

In 2013, deployment of portable body scanners is likely to become more widespread in the United States. We will closely monitor developments in this field and focus on the plans for European law enforcement organisations to use this new technology. Initially, the range and resolution of these scanners will be limited. However, the technology will improve, the range extended to allow the covert scanning of individuals on the street and the resolution will improve to reveal a more detailed image.

CCTV feeds will be monitored by automated analysis.

We have been monitoring the use of CCTV for a number of years and in 2012, we published Guidelines for the use of CCTV in the EU institutions and bodies. As usage increases, so does the amount of information to be processed. Video feeds from CCTV contain a wealth of information, provided the data controller has the resources to analyse the content.

To tackle this problem, law enforcement organisations are looking at methods to automate the analysis of CCTV video feeds. For instance, one of the objectives of the EU-funded INDECT project is to create a solution for intelligent observation of CCTV feeds and automatic detection of suspicious behavior or violence in an urban environment, with automatic feedback to law enforcement.

One issue for researchers to consider when working on projects such as INDECT is the potential impact of the tools and systems on the fundamental rights of privacy and data protection if the content is used further. In order to achieve an adequate balance between security and rights such as privacy in a project, it is advisable to take this balance into account at the outset.

Technical options such as anonymisation of data, limited retention periods and so on could be incorporated when research objectives and targets are defined. There is a risk that technology developed without these criteria could be difficult or impossible to operate in line with civil rights.

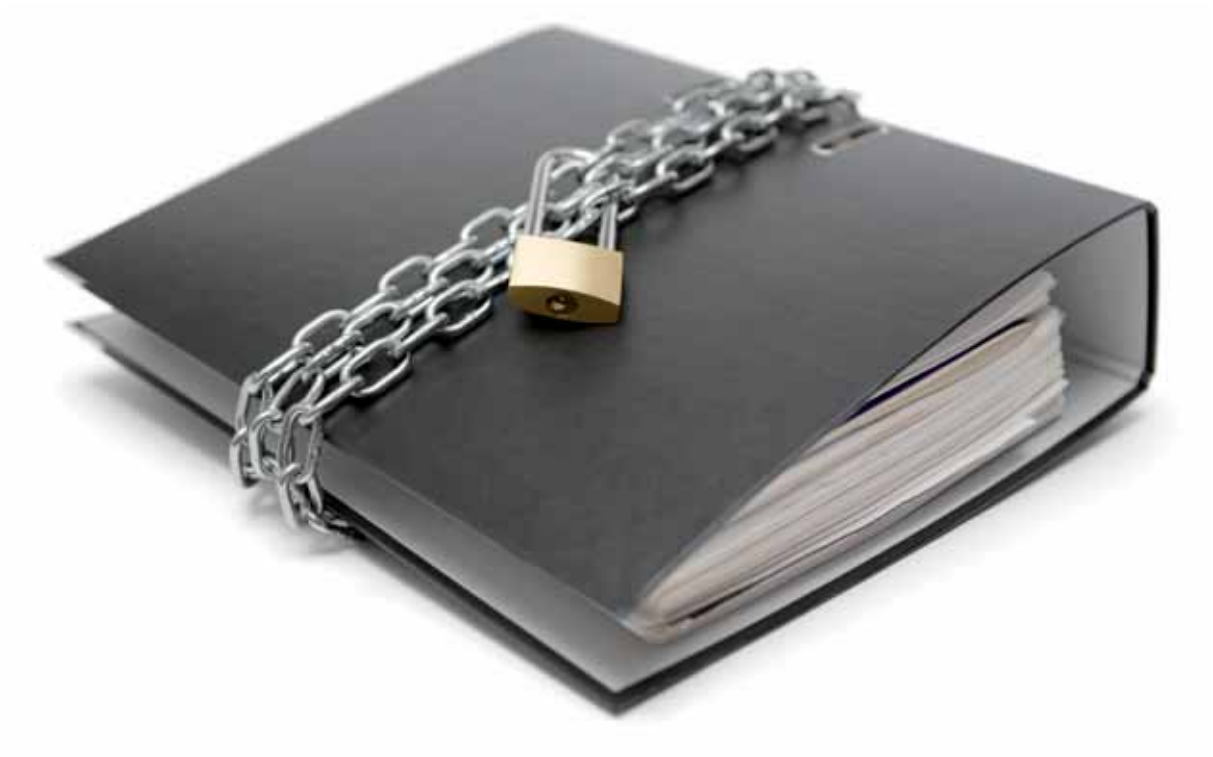
The use of drones will draw public attention.

Remotely piloted aircraft systems (RPAS), also known as unmanned aerial vehicles (UAV) or drones, were developed as military applications and this remains the predominant field of application. Recently, a 1.8 gigapixel camera-equipped drone which operates from an altitude of 5.3 kilometres and covers an area of 2.5 square kilometres has been documented on the internet[29].

Civil and scientific research applications with different characteristics are also becoming available. They mostly involve some form of remote sensing, monitoring or surveillance, based on images acquired via a high quality camera. The technology itself is maturing and it is likely that it will not be long before we see its widespread application. For instance, drones have been used at some sports events as a surveillance tool[30].

[29] http://www.liveleak.com/view?i=e95_1359267780

[30] http://rt.com/news/london-olympics-security-drones-007/



In an effort to examine the economic impact of this emerging technology, DG Enterprise of the Commission has launched a broad consultation on the future of civil RPAS applications in Europe. RPAS can deliver profitable commercial aerial services in various fields, such as in precision agriculture and fisheries, power or gas line monitoring, infrastructure inspection, communications and broadcast services, wireless communication relay and satellite augmentation systems, natural resources monitoring, media and entertainment, digital mapping, land and wildlife management, air quality control and management. The Commission foresees enormous potential for the technology and therefore, the need for legislation to safely integrate RPAS into European air space.

In contrast to fixed camera CCTV, RPAS fly. This means they potentially offer a unique perspective because they could monitor public spaces from the air. Their ability to move can be used to follow moving objects or people without having to merge multiple video feeds from separate fixed cameras.

Surveillance by RPAS is not always obvious and often quasi-anonymous. Although RPAS are unmanned, they are piloted manually and the images they capture can be fed into systems that analyse the footage. Technically, the images could potentially be stored for eternity. RPAS are a fast developing technology that challenges our understanding of surveillance and monitoring.

5.2.4. Other developments

The increased demand for privacy-preserving technology will lead to privacy standards, methodologies and tools for effectiveness and accountability.

The proposed general data protection Regulation requires data controller and processors to conduct impact assessments for data processing operations presenting specific risks to the rights and freedoms of data subjects. In addition, the proposal sets forth data protection by design and by default as mandatory practices to ensure adequate protection.

The first efforts towards the design of a *privacy impact assessment framework* at EU level were made for RFID applications[31]. The second attempt is being undertaken by the smart grid and smart meter industry and interested stakeholders. The PIAF[32] project, co-funded by the Commission, pub-

[31] http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

[32] «A Privacy Impact Assessment Framework for data protection and privacy rights" is a European Commission co-funded project that aims to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy and to the processing of personal data

lished its deliverables at the end of 2012. Included are a number of recommendations with regard to policy-making and practice on privacy impact assessments. The PIA standardisation attempt by the International Standards Organisation (ISO) is due in the foreseeable future.

Implementation practices of *privacy by design* approaches are emerging in many fields where privacy is at stake; identity and trust management, cloud computing services, smart meter and grids, biometrics, and many others. It would be useful if the knowledge gathered in research is tested and applied in production.

Privacy management and *privacy by design* will also be tackled by the ISO/IEC standardisation process. The Commission is to explore the possibility of a mandate to the European Standardisation Organisations (CEN/CENELEC/ETSI) for a standard on privacy by design in the security industry.

Data Breaches will continue to prove that no one is immune in the online environment.

As in past years, data breaches have affected a wide range of companies and organisations in 2012. Online international companies and important national companies where customer information was compromised have been involved in a large number of data breach cases. This proves once again, that no one is immune in the online environment.

Once a data breach is publically revealed, the consequences are usually serious for the entity responsible for protecting the information that was compromised. It is not unusual to hear that a data breach costs hundreds of thousands of Euro (or other currency) to rectify, as was the case with LinkedIn, a well-known social networking website for people in professional occupations, when the encrypted passwords of its users were published on the internet. LinkedIn announced that it paid close to 1 million USD (about 740.000€) in "forensic investigation and other recovery costs" for this data breach alone. No information is available on the cost to the users, the real victims of these breaches.

According to Verizon's 2012 Data Breach Investigations report, 97% of breaches were "avoidable through basic or intermediate controls." It is likely that this unfortunate trend will continue in coming years and that more efforts will need to be invested in basic security, in making the data controllers accountable, and in having them report data breaches to the affected individuals. Recent studies from the US suggest that one in four breach victims suffers identity theft; the resulting damage underlines the need to monitor these developments in order to ensure that respect for privacy and personal data protection is taken into consideration whenever possible.

6 INFORMATION AND COMMUNICATION

Our strategic objective

Develop an effective communication strategy

6.1. Introduction

Information and communication fulfils an important role in ensuring that our voice is heard and properly understood both within the EU administration and by the wider public. Our goal 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, we have adopted the key objective of developing a creative and effective communication strategy in our Strategy for 2013-2014. We have also enshrined our commitment to provide information to the public in Article 52 of our Rules of Procedure.

Through this strategy we aim to make the EDPS a point of reference at EU level for all matters falling

within our jurisdiction and also to ensure more **visibility** at institutional level and **raise awareness** both of our main activities (legislative opinions, prior check opinions, specific information to data subjects, training of EU data protection officers) and of data protection in general.

Although significant progress has already been made, awareness of our role and mission at EU level needs to be raised further and our communication activities are all the more important in achieving this.

Our increased visibility at institutional level is relevant for our three main roles i.e. the supervisory role in relation to all EU institutions and bodies involved in the processing of personal information; the consultative role in relation to those institutions (Commission, Council and Parliament) that are involved in the development and adoption of new legislation and policies that may have an impact on the protection of personal information; and the cooperative role in relation to national supervisory authorities and the various supervisory bodies in the field of security and justice.

Indicators such as the number of information requests received from citizens, media enquiries and interview requests, the number of subscribers to the newsletter, followers of the EDPS account on Twitter, as well as invitations to speak at conferences and website traffic, all support the view that we are successful in becoming a point of reference for data protection issues at EU level.

6.2. Communication 'features'

The evolution of our 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

The communication policies and activities of most other EU institutions and bodies generally address EU citizens as a whole. Our direct sphere of action is more distinct. Our primary focus is on our stakeholders – EU institutions and bodies, data subjects in general and EU staff in particular, EU political stakeholders and those in the data protection community. As a result, our communication policy does not need to engage in mass communication. Instead, awareness of data protection issues among EU citizens in the Member States depends essentially on a more indirect approach, via data protection authorities at national level, for instance.

Nonetheless, we do communicate with the general public, via a number of communication tools such as our website, Twitter, newsletter, awareness-raising events and we regularly interact with interested parties – through study visits, for instance – and participate in public events, meetings and conferences.

6.2.2. Language policy

To be effective, our communication policy needs to take into account the specific nature of our organisation's field of activity. Data protection issues are often perceived as fairly technical and obscure for non-experts, therefore, the language in which we communicate must be adapted to counter this. For our information and communication activities to attract a diverse audience, clear and accessible language which avoids unnecessary jargon is vital. In 2012, as in past years, we have made continued efforts in this regard, particularly when communicating with the general public and general press. Our over-riding aim in this context has been to correct the excessive legal and technical image of data protection. Our Strategy 2013-2014 therefore commits us to communicate in ways that are easy for the public to understand.

Of course, when we address more informed audiences, such as data protection specialists, EU stakeholders and so on, more specialised language is appropriate. We appreciate the value of using different communication styles and language patterns to communicate the same news according to the audience.

Our press and communication activities are offered in at least three languages – English, French and German – and this has been so since 2010. Our overall aim is to reach the widest possible audience.

6.3. Media relations

To cultivate an image of a reactive and reliable partner and to promote the EDPS as an independent point of reference for data protection at EU level, our objective has been to continue building and maintaining regular contacts across the media.

We aim to be as accessible as possible to journalists so that the public can follow our activities. We regularly interact with the media through press releases, interviews and press events. The handling of regular media enquiries allows further contact with the media.

6.3.1. Press releases

In 2012, our press service issued 17 press releases. Many of these related to our **supervision** and **consultation** work, especially **new legislative opinions** directly relevant to the general public. Among the issues covered by these press releases were the EU data protection reform strategy, the report on our general compliance survey, financial markets, ACTA, smart meters, driver cards for professional drivers, video surveillance, open data package, amendment to the EURODAC regulation, Commission v. Austria, cloud computing, and our guidance policy for DPOs.

Press releases are published on the EDPS website and on the Commission inter-institutional database of press releases (RAPID) in English, French and German. They 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 2012, the EDPS and the Assistant EDPS gave 40 direct interviews to journalists from print, broadcast and electronic media throughout Europe and the US.

The resulting articles featured in international, national and EU press, both mainstream and specialised (such as in information technology issues, 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 in the field of privacy and data protection. They also addressed more specific issues that made the headlines in 2012, including ACTA, smart meters, cloud computing, EURODAC, the review of the EU legal framework for data protection, privacy concerns related to social networking, digital rights, data retention and security.

6.3.3. Press conferences

In 2012, we held three successful press events. A press breakfast on 7 March on the EU data protection reform package; a press conference on 20 June to present our Annual Report for 2011, which was also an opportunity to discuss the reform proposals further and, another press breakfast on 16 November on cloud computing.

These events were occasions for journalists to pose questions to Peter Hustinx, EDPS, and Giovanni Buttarelli, Assistant Supervisor on these issues specifically as well as in the wider context of EU data protection and its future challenges.

6.3.4. Media enquiries

In 2012, the EDPS received some 46 written media enquiries that included requests for EDPS comments and for clarification or information. Media attention spread across many issues – cookies, eHealth, PNR, EURODAC, CCTV for instance – but we had repeated requests on EU data protection reform, smart meters, cloud computing and ACTA.

6.4. Requests for information and advice

In 2012, we dealt with 116 enquiries from the public or interested parties for information or assistance. While this figure is lower than 2011, it is still 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 such as factsheets and the use of Twitter, mean that we are

becoming more efficient in getting our messages across.

Requests for information come from a wide range of individuals and parties, ranging from stakeholders operating in the EU environment and/or working in the field of privacy, data protection and information technology (such as law firms, consultancies, lobbyists, NGOs, associations, universities, etc.) to citizens asking for more information on privacy matters or requiring assistance in dealing with the privacy problems they have encountered.

The majority of these requests in 2012 were actually complaints from EU citizens on matters for 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 other relevant EU institution, body or agency.

Other categories of information requests included enquiries about EDPS activities, role and missions, EU data protection legislation and its review, cloud computing, ACTA, eHealth, cookies and ePrivacy, biometrics, consent, large-scale IT systems such as SIS and EURODAC, related data protection issues within the EU administration, such as processing activities by EU institutions, bodies and agencies.

6.5. Study visits

As part of the efforts to increase 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 2012, we were visited by the representatives of the data protection authorities of Norway and the FYROM. On 17 April, we welcomed the FYROM delegation to our offices and talked to them about video surveillance, coordinated supervision and privacy in the workplace. The Norwegian delegation, on 3 December, was keen to hear from us about the EU data protection reform, the Article 29 Working Party and our supervisory role in the EU public sector.

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 or Assistant Supervisor, press releases, newsletters, event information and so on – are all available through this platform.

Web developments

2012 was a very fruitful year in our web development activities. The most prominent of these was the overhaul of the supervision and consultation sections. In order to improve the search function and navigation through thematic categories, a filtering system was introduced. Visitors should now find it easier to look for documents on the different topics covered.

A new search function was also developed for the EDPS register, allowing the search for documents not only on a given topic, but also by specific institutions on specific dates.

In 2012, we launched a dedicated DPO Corner on our website. This new feature is in extranet form with password access and serves as a communication platform for all DPOs of European institutions and bodies. Within a few months of going live, the DPO Corner has received a great deal of positive

feedback as a forum for simplifying contacts between us and DPOs.

Other website developments included:

- implementing the RSS feed feature;
- further improvement of the electronic complaint submission form introduced in 2011;
- graphic changes on the homepage.

We will maintain our efforts to improve website performance in 2013.

Traffic and navigation

An analysis of traffic and navigation data shows that in 2012, we had a total of 83 618 new visitors to our website, which is a significant increase from 2011 (+ 27.5%). The total number of visits in 2012 was 179 542, an increase by 40.4% compared to 2011. In October and November 2012, the number of visits exceeded 18 000 per month.

From 1 January 2013, these figures will be one of the 10 key performance indicators for the EDPS (see above, section 1.2 on the EDPS Strategic Review and our 'Strategy 2013-2014' document on our website).

After the homepage, the most regularly viewed pages were consultation, press and news, publications and supervision. 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 40% 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 attention to additions 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 details upcoming and recent conferences and other events, as well as speeches by the Supervisor or Assistant Supervisor. The newsletter is available in English, French and German on our website and readers are included on our mailing list via an online subscription feature.

Five issues of our newsletter were published in 2012, with an average frequency of one issue every two months (July and September are excluded). The number of subscribers rose from 1 750 at the end of 2011 to 1950 in 2012. Subscribers include members of the European Parliament, staff members of 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 media service that has worldwide popularity. It allows users to send and read text-based posts of up to 140 characters, known as tweets. It has been described as *the SMS of the Internet*, although tweets are in principle available for everyone to read.

In 1 June 2012, the EDPS joined the Twitter community (@EU_EDPS), our first step towards online interactive communication. Prior to this, we had a passive presence on Twitter, as both the EDPS and data protection related topics regularly appeared in Twitter messages.

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 remains manageable with limited resources.

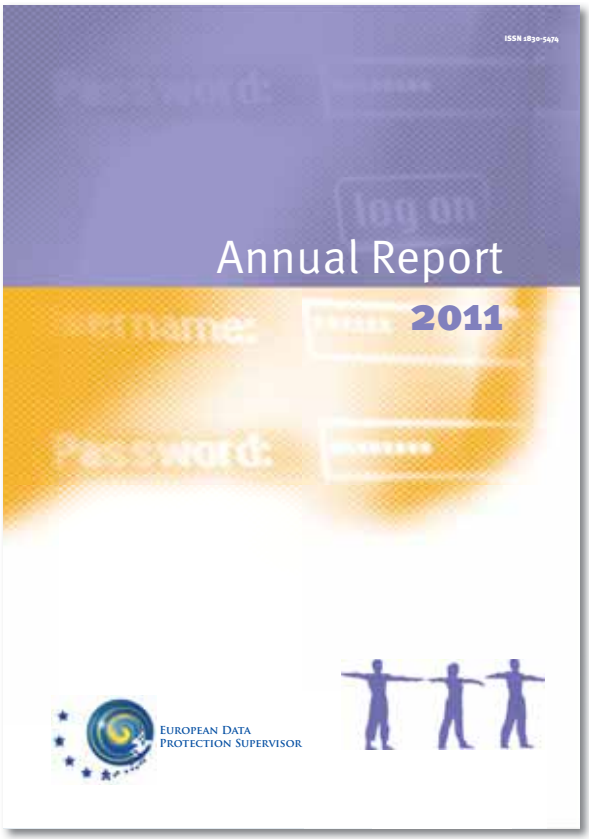
In line with our policy, our Tweets have centred on our

- press releases;
- new opinions;
- new publications;
- speeches and articles;
- videos;
- links to interesting articles regarding EDPS and data protection;
- upcoming participation in events.

By the end of 2012, we had tweeted 83 times, were following 150 other Twitter users and had 312 followers. In 2013, we will review the success of our Twitter account and revise and update our Twitter policy as appropriate.

6.7. Publications

6.7.1. Annual Report

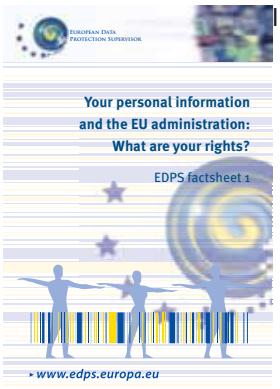


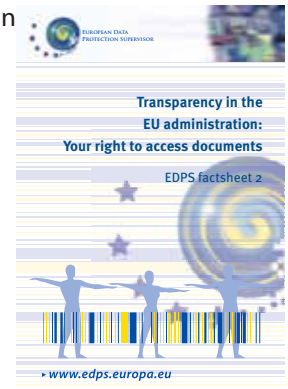
The EDPS annual report is a key publication for us. It is an account of our work in the main operational fields of supervision, consultation and cooperation from the reporting year and also sets out the main priorities for the following year. In addition, it describes what has been achieved through external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

The report may be of particular interest to various groups and individuals at national, European and international levels – data subjects in general and EU staff in particular, the EU institutional system, 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 at EU level.

The Supervisor and Assistant Supervisor presented the 2011 Annual Report to the LIBE committee in the European Parliament on 20 June 2012. The main features of the report were also presented at the press conference on the same day.

6.7.2. Thematic publications





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

Relating to data protection issues of strategic importance for the EDPS, we aim to publish targeted information as guidance for the general public and other interested parties. Other themes for factsheets currently include *Transparency in the EU administration and your rights to access documents*, ePrivacy, smart meters, data breaches, video surveillance and the supervisory role of the EDPS. We aim to publish as many of these as possible on our website by the end of 2013 in English, French and German.

6.8. Awareness-raising events

We are keen to seize relevant opportunities to highlight the increasing relevance of privacy and data protection and to raise awareness of the rights of data subjects as well as the obligations of the European administration in this area.

6.8.1. Data Protection Day 2012

The countries of the Council of Europe and the European institutions and bodies celebrated the fifth European Data Protection Day on 28 January 2012. This date marks the anniversary of the adoption of the Council of Europe Convention on the protection of personal data (Convention 108), the first legally binding international instrument in the field of data protection.

The day is the perfect opportunity to raise awareness among EU staff and other interested persons about their data protection rights and obligations. We circulated a video message from the Supervisor

and Assistant Supervisor to institutional stakeholders and on our website, on privacy and data protection as fundamental rights which also highlighted the everyday processing of personal information and the associated risks.

As we do every year, we once again offered our support to the awareness raising efforts of DPOs in the EU institutions and bodies.

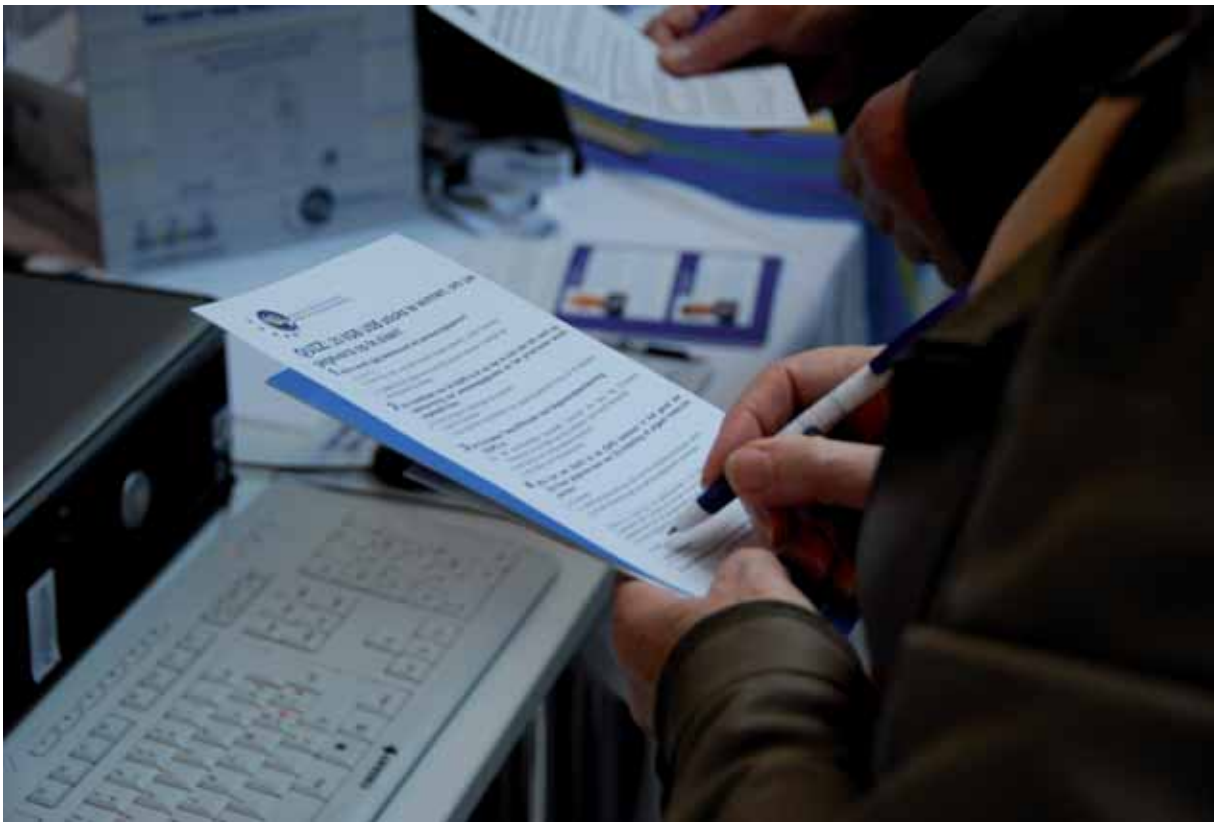
We also took part in the events organised by the Commission and the Council, as we do every year. On 25 January, the Supervisor and Assistant Supervisor spoke at a breakfast meeting with the DPO and DPCs of the Commission.

We also participated in other events, such as the fifth international conference on *Computers, Privacy and Data Protection* on 25-27 January in Brussels, which serves as a bridge for policymakers, academics, practitioners and activists to discuss emerging issues of privacy, data protection and information technology. The European data protection framework, copyright enforcement and privacy, privacy and the trans-border flow of personal data were just some of the panels in which we participated, while the Supervisor made closing remarks.

6.8.2. EU Open Day 2012

On 12 May 2012, we once again participated in the annual Open Day at the EU institutions. 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.

EDPS colleagues welcomed visitors to our stand in the main building of the European Parliament and answered questions on the data protection and privacy rights of EU citizens. Visitors could also take part in our fun data protection quiz and take away some information material. The infra-red camera linked to a large screen was a major attraction at our stand. Although there was no direct link to processing of personal information, it was a striking and thought-provoking way to highlight the potential privacy risks posed by new technology.



7 ADMINISTRATION, BUDGET AND STAFF

Our strategic objective

Improve the use of 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 the climate of economic austerity, we imposed severe budget cuts on ourselves for a second time in 2012. In order to do *more with less* we put in place new control mechanisms such as quarterly budget implementation reviews and three levels of planning (monthly, annual and strategic) which allowed better monitoring of activities as well as a more efficient allocation of resources.

Strategic thinking, better planning, more efficient allocation and use of resources also dominated our agendas in 2012 in a much wider sense.

In late 2012, we moved from our old premises in Rue Montoyer 63 to a new address, Rue Montoyer 30. As before, we rent this new office space from the European Parliament under an inter-institutional agreement, whose services continue to assist us with all matters related to IT, infrastructure and logistics. This successful and long delayed move was the result of brainstorming activities and the work of an internal taskforce, which in turn, were part of our overall Strategic Review.

We also achieved substantial improvements in the efficiency of the HR function in 2012 by integrating Sysper2 (a personnel file management system) and MIPs (a missions management system), two systems mainly developed for use by the European Commission.

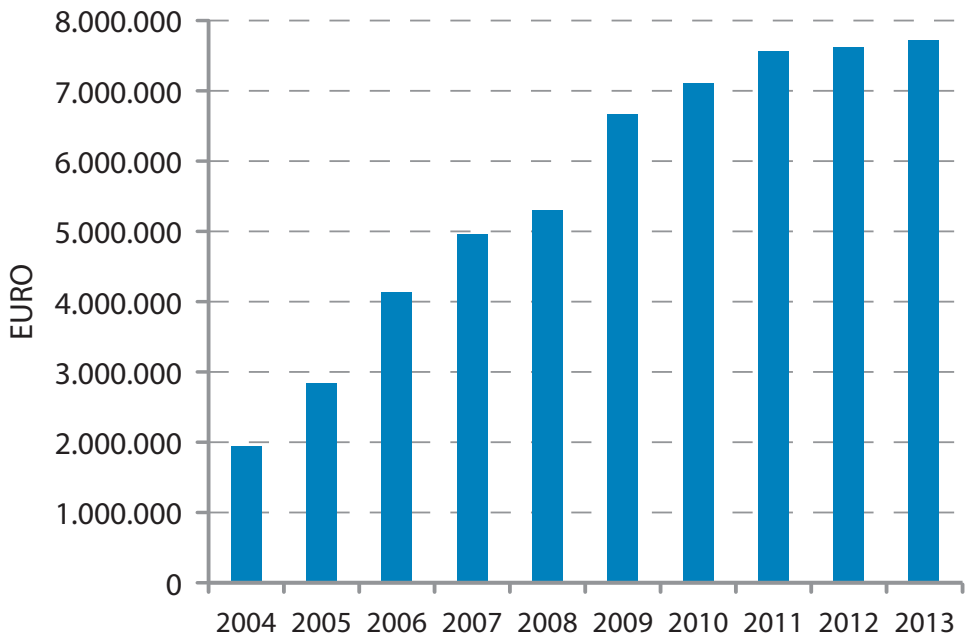
In addition, better allocation and control of financial resources led to a significant budget implementation rate of around 90%.

In line with the Annual Management Plan 2012, we established a procurement function. This allowed the launching of procurement procedures that are fully managed by us.

7.2. Budget, finance and procurement

7.2.1. Budget

EDPS – Budget evolution 2004-2013



In 2012, the allocated budget for the EDPS was EUR 7 624 090, which represents an increase of 0.79% on the 2011 budget. This is actually a nominal reduction, taking into consideration the inflation rate foreseen at 1.9% for 2012.

In a period of economic austerity and in line with other EU institutions and Member States, we made considerable efforts to consolidate our budget significantly. This is a particularly difficult task for a small budget. Unlike other long-established EU institutions with comparatively large resources, ours is a small institution in its growing phase. We were able to reduce our budget by means of a fundamental redeployment of resources and by identifying negative priorities.

To cope with the scenario that combines both a budget reduction and an increase of responsibilities, we have implemented a culture of accrued optimisation in the use of resources, in other words, *do more with less*. We have improved our quarterly budget implementation review that was implemented in 2011 and this has proved to be the key tool for the efficient use of our limited resources.

As a result of this exercise, our budget implementation rate has improved substantially: from 76% in 2010, to 85% in 2011 and to 90% foreseen for 2012.

7.2.2. Finance

The Statement of Assurance from the European Court of Auditors concerning the financial year 2011 (DAS 2011) did not raise any concerns or recommendations for the EDPS. Nevertheless, within the context of sound financial management and with a view to improve the reliability and the quality of our financial data:

a) a charter of tasks and responsibilities of authorising officers by delegation and sub-delegation was prepared for adoption in January 2013;

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

c) the use of the mission application MIPS, for better control and transparency was implemented;

d) in light of a possible future creation of the European Data Protection Board administratively linked to the EDPS, a new title III was drawn up and included in the EDPS budget (no additional appropriations were requested at this stage);

e) an internal procedure for reimbursement of representation expenses was adopted.

Assistance from the Commission in finance matters continued in 2012, particularly in relation to accountancy services, as the Accounting Officer of the Commission is also the Accounting Officer of the EDPS.

7.2.3. Procurement

In order to gain greater autonomy in the field of procurement, we adopted our own *Step-by-step procurement Guidelines for low value* contracts in June 2012.[33]

As a result, two procedures were launched in 2012. The first one in June was a competitively negotiated procedure for video production. The second, in December, was a negotiated procedure for IT assistance. The total amount for the associated contracts to be signed was EUR 73.200.

7.3. Human resources

7.3.1. Recruitment

The EDPS is a comparatively small EU institution and our staff is characterised by versatility and a high workload. The result is that any departure of staff is problematic because it is not easy to find a replacement and until a new colleague is in place, the already heavy workload of the other colleagues is increased. Recruiting the right person as quickly as possible is, therefore, paramount and the HR team takes great care over this task in order to minimise the impact of such departures.

A policy of moderate but sustainable growth for the EDPS was put in place by the Council and the European Parliament in the Financial Perspectives for 2007-2013. This policy has allowed our institution to increase the staff with two new members every year until 2013, when conclusion of the establishment plan was foreseen. New colleagues were immediately assigned to assist with the growing workload which has been the result of the increasing importance of data protection and the visibility of our institution, as well as the entry into force of the Lisbon Treaty.

After the general competition on data protection of 2009, we recruited extensively in the following years. The reserve lists of the data protection competition are now practically exhausted. We have also received a significant number of transfer applications from EU officials in other institutions, which demonstrates the growing visibility of the EDPS as an attractive employer.

In 2012, we recruited seven officials, three of whom were to staff the new IT policy sector (see 7.3.5), two for the HRBA Unit following one departure and an internal reorganisation of the unit and one each for the two existing data protection units.

In addition to these EU officials, we recruited one seconded national expert (S&E team) and three contract agents (S&E and P&C teams). In total, either because of staff turnover or new incorporations, the HRBA Unit organised the recruitment of eleven new staff members in 2012.

The chart below shows the significant growth of the organisation over the last three years, following the creation of three new sectors (I&C, OPS and ITP). The units (S&E, P&C and HRBA) have not experienced significant reductions in personnel.

7.3.2. Professionalising the HR function

Following the adoption of several manuals and decisions in 2011, the HR team issued its first report on metrics, past and planned activities, which was submitted for the consideration of the Management Board of the EDPS in 2012.

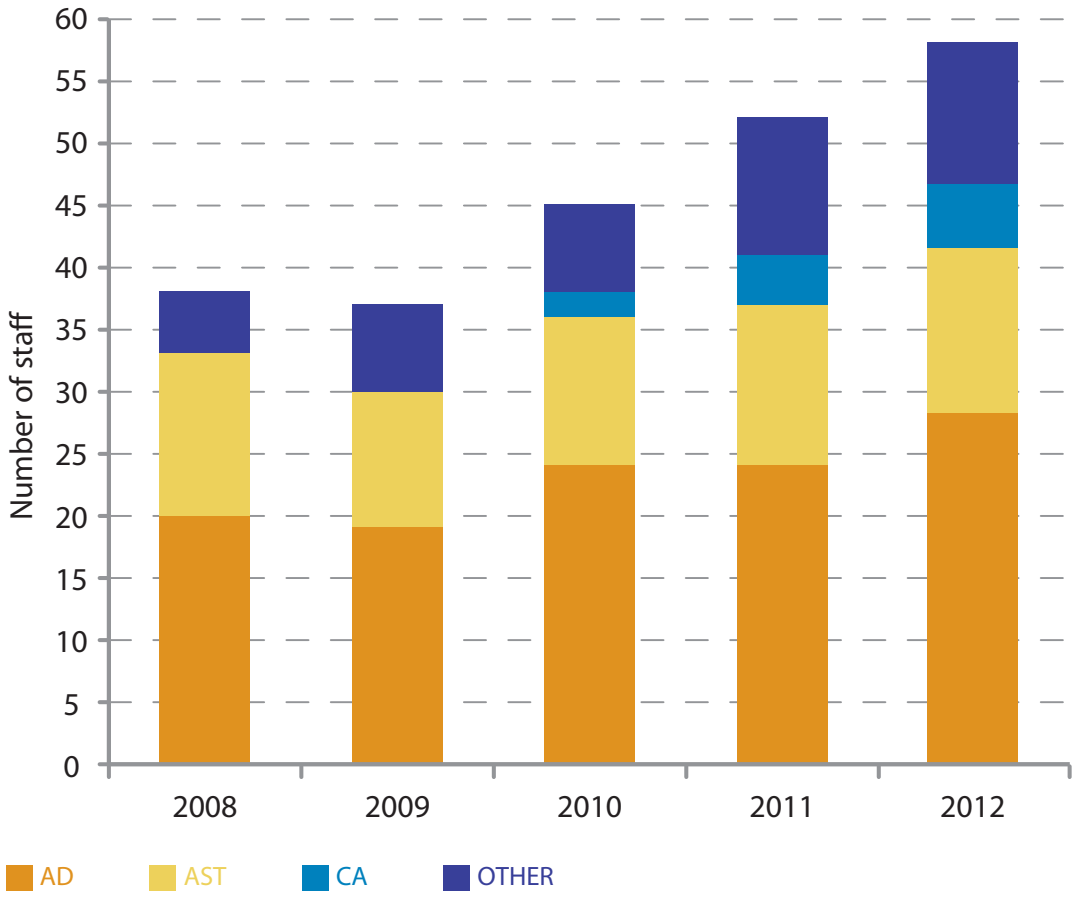
Furthermore, our considerable efforts and negotiation with several European Commission departments finally resulted in the integration of Sysper2 family. The result is simplification and a professionalising of the HR function within our compact institution.

In preparation for a visit of the internal auditor, the HR team carried out an extensive screening of all its activities. As a result, decisions, workflows, processes, record management practices, etc. were thoroughly analysed for each activity, revealing any inconsistencies or inefficiencies that have resulted from the growth of the institution over the years. Many of these were addressed in 2012 and the remainder will be dealt with in 2013.

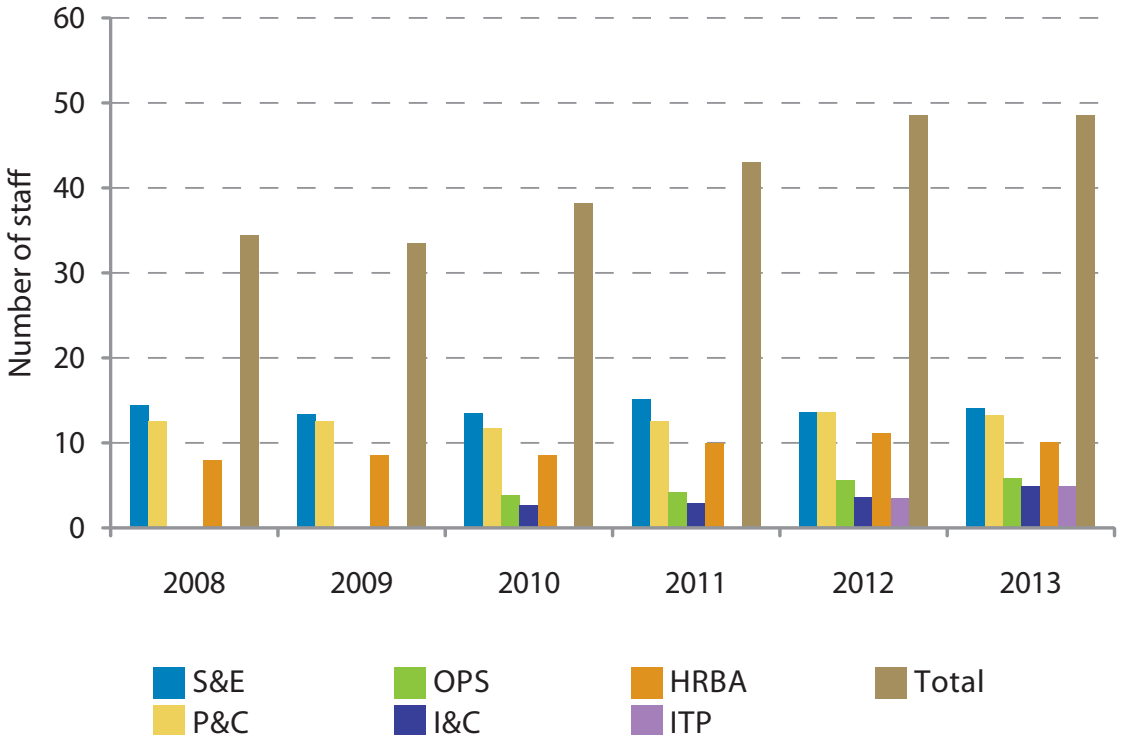
As a result of this screening, several EDPS implementing decisions were updated and sixteen data protection notifications were sent or updated.

[33] To be amended according to the new Financial Regulation entered into force on 1 January 2013.

EDPS – Staff evolution by category



EDPS staff Evolution 2008-2013



7.3.3. Traineeship programme

In 2012, our organisation continued to invest in the traineeship programme which was established in 2005. This programme offers recent university graduates the opportunity to put their academic knowledge into practice. We offer opportunities to acquire practical experience in our day-to-day activities in the operational units and also in the HRBA units, the I&C and ITP sectors.

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 which is available on our website.

All trainees, whether remunerated or not, contribute to both theoretical and practical work and gain useful first-hand experience. Historically, the trainees were recruited in the P&C, S&E and HRBA units. In 2012, in addition to those trainees, the EDPS recruited trainees in the information and communication sector and in the newly created IT policy sector.

As of October 2012, due to additional space in the new building, we may consider additional non-remunerated trainees.

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 enable us to benefit from the skills and experience of such staff and help to 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).

7.3.5. Organisation chart

The EDPS organisation chart was updated in 2012. A new sector, *information technology policy* was created on 1 April 2012. This sector is composed of two posts transferred from the S&E Unit, one post from the P&C Unit and a new post agreed by the budgetary authority for 2012, which was used for the recruitment of the Head of Sector. A new post will reinforce this sector in 2013.

The increasingly important role of coordinators was also recognised. We continued to build on this function in 2012 by confirming existing coordinators, appointing new coordinators and clarifying their functions and responsibility, as well as the use of the terminology *head of activity*. This resulted in the designation of six heads of activity (three in S&E Unit, two in the P&C Unit and one in the HRBA Unit).

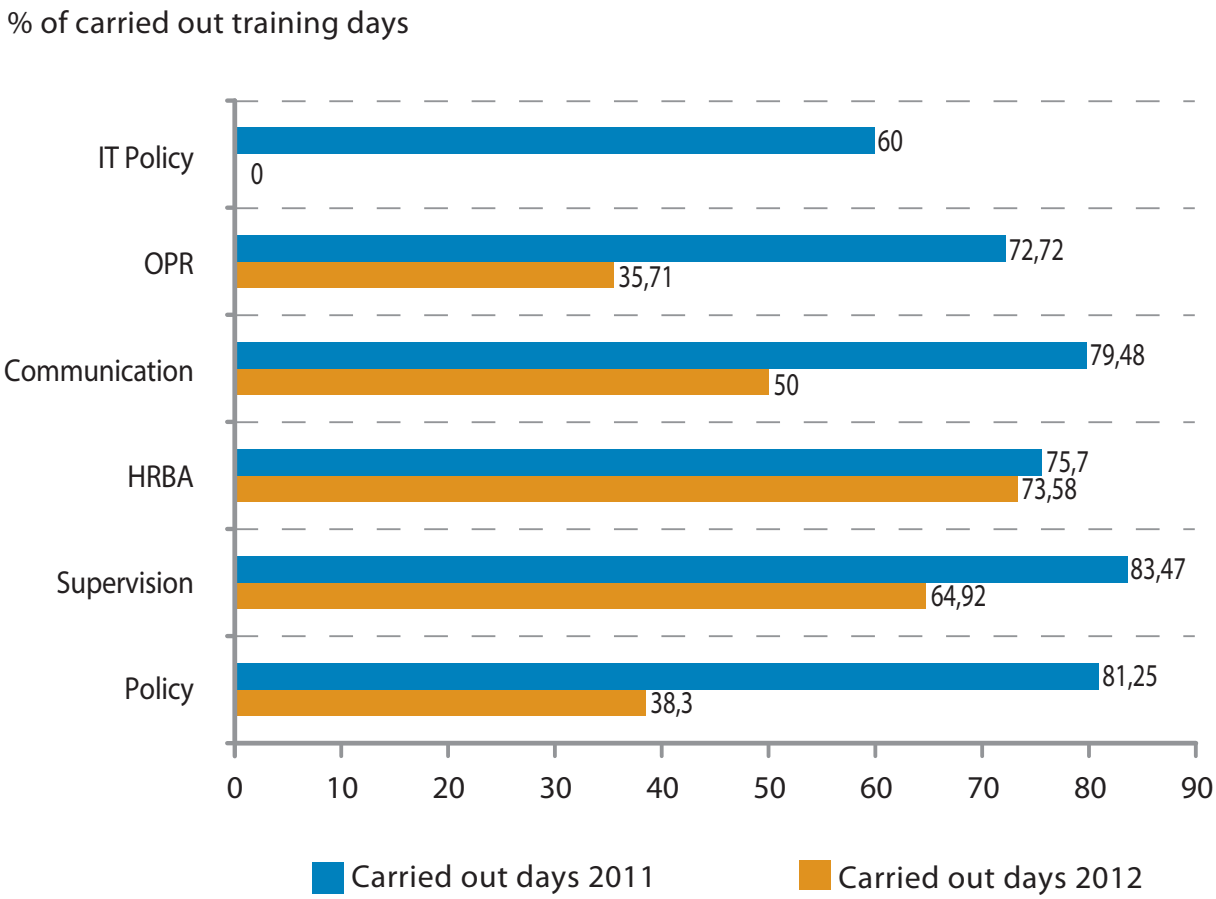
7.3.6. Working conditions

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 the limited flexibility provided by this legal framework, the HR team endeavours to make them as attractive and flexible as possible for our staff, in particular for those with family responsibilities.

The flexitime scheme is highly appreciated by staff. Currently 99,5 % of staff members introduce their working hours in Sysper 2. 10% use flexitime only to benefit from flexible working hours while the rest of the users use it not only to have flexible hours but also to recover overtime (in days or half days).

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

Our decision on teleworking, largely inspired by the similar decision at the Commission, was adopted in July 2012 following many discussions between management and the Staff Committee. The teleworking scheme was subsequently launched as a pilot project in September 2012. The pilot phase will end in February 2013 and adjustments will be made if necessary. 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 some reason but is able to work nonetheless (maximum of twelve days per year).

During the pilot phase two staff members made use of structural teleworking whereas nineteen requests for occasional teleworking were granted.

7.3.7. Training

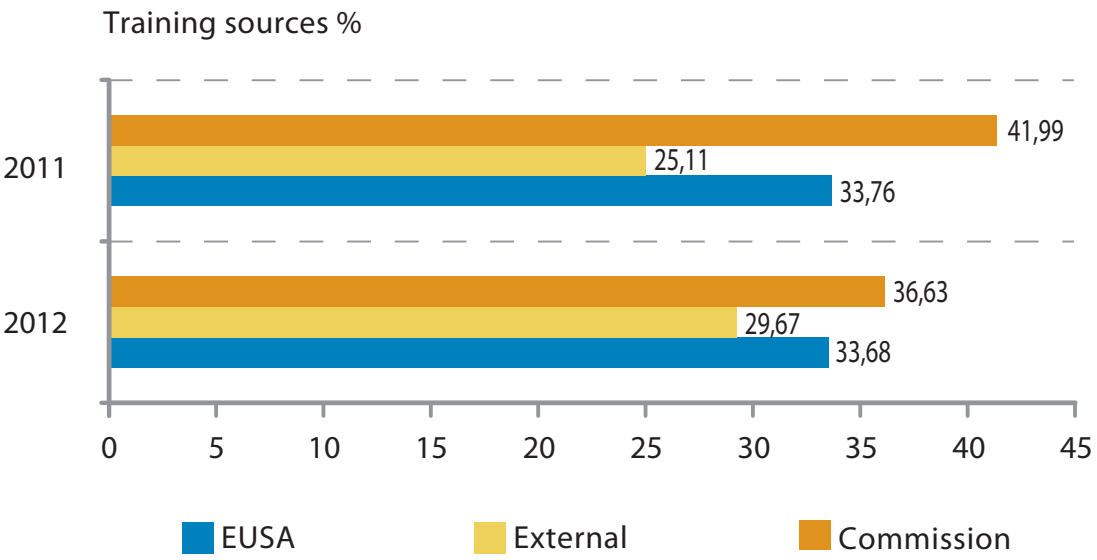
Training and career development at the EDPS improved substantially in 2011, both in terms of the number of courses followed and the diversity of training courses. This trend continued in 2012 as staff became more familiar with offers contained in Syslog 2 (a system managing the Commission training catalogue and training course applications).

As a result, the number of training days increased substantially (+ 60.51% from 2011). The percentage of actual training days compared to days estimated in training maps at the beginning of the year grew also from 56.82 % in 2011 to 77.59 % in 2012.

The three main training providers for our institution are the Commission, the European School of Administration (EUSA), which represents one third of the total training courses taken up by EDPS staff, and other external service providers such as European Training Institutes which provide some specific training courses, particularly important for legal officers. The graph below shows the evolution.

In 2012, there were two tailor-made courses offered to our staff: a second session of *First steps in management* provided by the European Administration School, and a course specifically for the Supervision Unit called *How to deal with interviews during an inspection*. The latter (which has been followed and recommended by staff of the French DPA, the CNIL) was particularly relevant in the context of our supervisory powers (Article 47.1 of Regulation 45/2001). Twelve staff members took part in each course.

Management training for members of the new management team continued in 2012 and this resulted in tangible improvements in terms of planning, coordination and implementation of policies at the Director's meeting.



7.3.8. Social activities

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 Unit, 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 2012, several social activities were organised with full involvement of the Staff Committee of the institution.

In our new premises a social room, *The Cloud*, has been made available to staff where they can get together for a coffee, lunch or social activities. Meetings of the Staff Committee also take place here.

7.4. Control functions

7.4.1. Internal control

The internal control system, effective since 2006, manages the risk of failure to achieve business objectives. In 2012, we extended the list of implementing actions to ensure more efficient internal control of the processes in place. By way of example, a revised version of all job descriptions, internal rules of procedure (Article 46.k of Regulation (EC) 45/2001), presentation of units' activities to all staff, a case manual on access to documents and a new risk register were some actions which were adopted to implement internal control standards (ICS).

A revised decision on ICS will be adopted in January 2013 to simplify the approach, increase ownership and strengthen their effectiveness.

Following the adoption of an annual management plan at the beginning of 2012, we adopted a decision on risk management in July 2012 – contemporary tools which help identify risks and possible courses of action. Risk management involves more than an assessment of risks, it also requires that we put in place controls and actions which must then be followed-up. Thus, we have included risk management as an essential element of our overall strategy of *total quality management* (TQM).

We have taken note of the annual activity report and the Declaration of Assurance signed by the Authorising Officer by delegation. Overall, we con-

sider that the internal control systems put in place provide 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.

Further to the audit report of November 2011 concerning prior checking opinions, administrative measures and inspections, a report was issued in April 2012 with a number of recommendations for follow up.

In June 2012, further to this specific audit, the IAS issued an Advisory Report on the Inspection process at the EDPS. The objective of this advisory engagement was to provide recommendations for further improvement in the EDPS inspection process. The areas for improvement included: strategic approach, the inspection processes, resource management and monitoring measures put in place by us in order to run the process effectively and effectively.

In May 2012, the IAS issued the Annual Internal Audit Report (ARIA – Article 86 (3) of the Financial Regulation) for 2011, which summarised the internal audit activity in 2011 at the EDPS.

Of the follow up of the six pending open recommendations of previous audits, two were closed by the IAS and the other four are likely to be closed in the course of 2013.

As the IAS and EDPS have a common interest in the area of audits, a Memorandum of Understanding (MoU) to allow both organisations to fulfil their roles in the most efficient way was signed in May 2012. The MoU was concluded with full regard to their respective rights, obligations and independence as laid down in their constitutive documents.

A Service Level Agreement (SLA) between the IAS and the EDPS was signed at the same time. Since September 2004, the date of appointment of the Internal Auditor of the Commission as Internal Auditor of the EDPS, the IAS has provided audit services in the framework of the Inter-Institutional Agreement between the European Parliament, the European Commission and the EDPS. As the inter-institutional agreement with the Commission will expire in December 2013, this SLA will act as a self-standing document on which to base such audit services in the future.

Finally, the IAS mission charter was also signed in May 2012. This Charter sets out the mission, objectives, reporting and working arrangements that are essential to the proper fulfilment of the IAS' role towards the EDPS.

7.4.3. External audit

As an EU institution, 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 2011, the questions posed by the Court were answered satisfactorily by the EDPS. In June 2012, a letter to the EDPS from the Court stated that there were "*no observations resulted for the audit work carried out*".

The Court of Auditors (Article 143 of the Financial Regulation) stated that it did not identify any significant weakness in the areas it audited and that the measures implemented (social allowances) as a result of its audit, were effective. We took note of the Court's analysis and intend to continue improving our system for timely monitoring and control.

In January 2012, the EDPS Director attended the discharge meeting at the Budgetary 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 2010.

7.5. Infrastructure

The offices of the EDPS are located in one of the buildings of the European Parliament. As a result of an inter-institutional cooperation agreement, the Parliament also supports us with IT and infrastructure.

After long and careful preparation in 2011 and most of 2012, we finally moved to our new offices at Rue Montoyer 30 in Brussels. Close collaboration with the European Parliament services ensured efficient planning and a smooth move in October 2012, with minimal disruption to our work. We took the opportunity of the move to invest and upgrade in some IT material, such as the acquisition of a video-conference system which should lead to savings in mission expenditure, as the technology allows participation in external meetings from our premises.

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

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 with 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.

However, in 2012, in view of our imminent move to new offices, the European Parliament preferred a revision of the General Administrative Agreement that it has with us, together with the related 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 these texts. Technically agreed in 2012, the General Administrative Agreement and its annexes will be signed in early 2013. This administrative cooperation is vital for us as it increases efficiency and allows for economies of scale.

In 2012, 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 and various European Parliament services (IT services, particularly with arrangements for the maintenance and development of our website; fitting out of the premises, building security, printing, mail, telephone, supplies, etc.). This cooperation mainly 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. A good example of the results of this inter-institutional cooperation is the work with DG DIGIT and DG HR of the Commission and DG DIGIT and PMO which made our incorporation of Sysper2 and MIPs families in 2012 possible.

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*.

On 22 October 2012, the HRBA team visited the Court of Auditors to participate in a series of workshops on good practices in the fields of HR, Budget/Finance and Administration. As a result of these discussions, new working methods and ideas will be implemented in 2013.

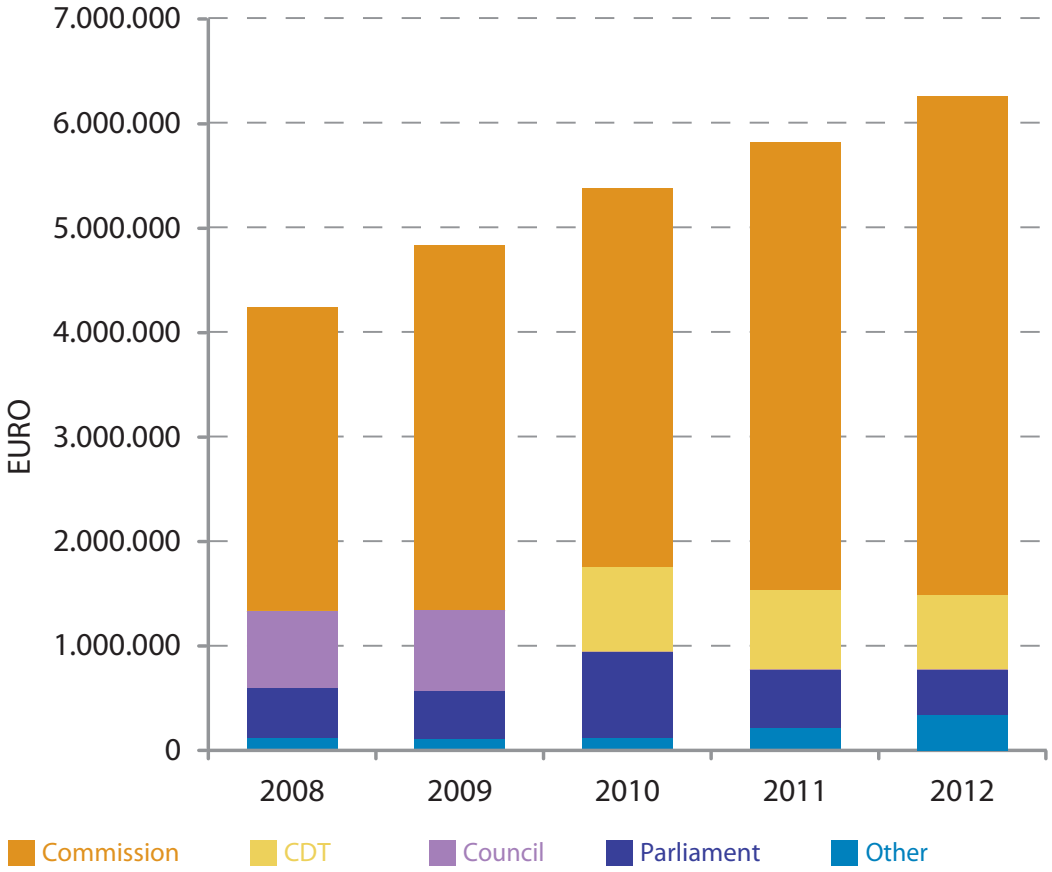
7.6.2. Document management

During 2012, we customised a document and records management system, incorporating case management. This document and records management system is able to store documents and records grouped together in case files for all our activities. Case files are classified according to a filing plan.

The system includes features such as sophisticated access control, mail registration, retention schedules, ability to set legal holds, document versioning, subject tagging, full text and database search functionality, audit trails, reporting and workflows.

The system is expected to be deployed in 2013.

EDPS budget execution through inter-institutional cooperation



8 EDPS DATA PROTECTION OFFICER

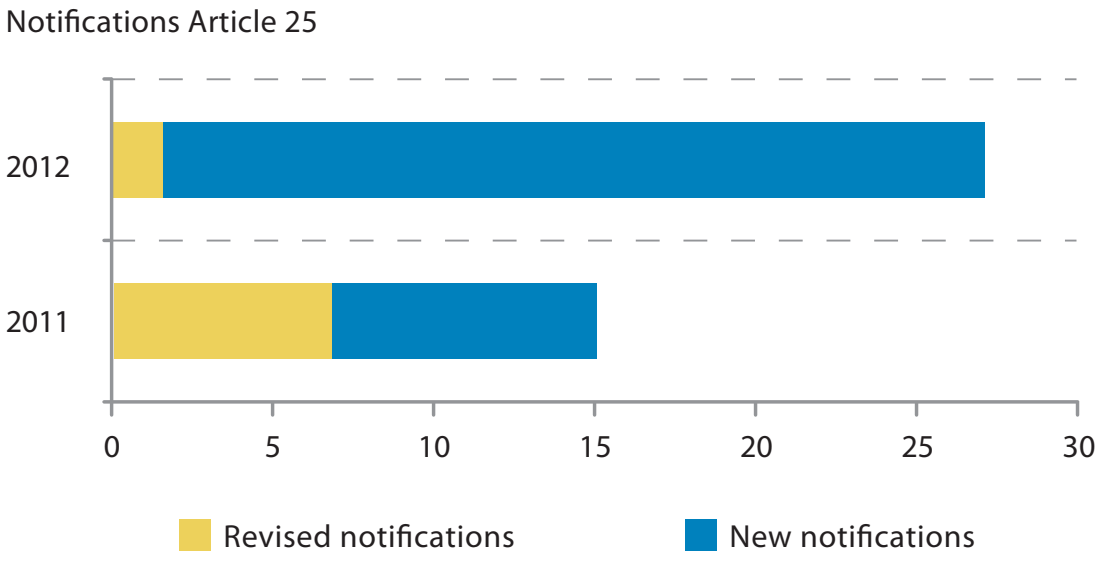
8.1. The DPO at the EDPS

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 particularly aware and sensitive about data protection issues and delivering solutions that can serve as benchmarks for other institutions.

To strengthen this independence and enhance her expertise, the EDPS DPO took the IAPP (International Association of Privacy Professionals) training course, recommended in the DPO paper on professional standards issued by the DPO network[34] and was successful in becoming a Certified Information Privacy Professional/Europe (CIPP/E). The DPO also attended the IAPP Congress in November 2012 to further consolidate her expertise.

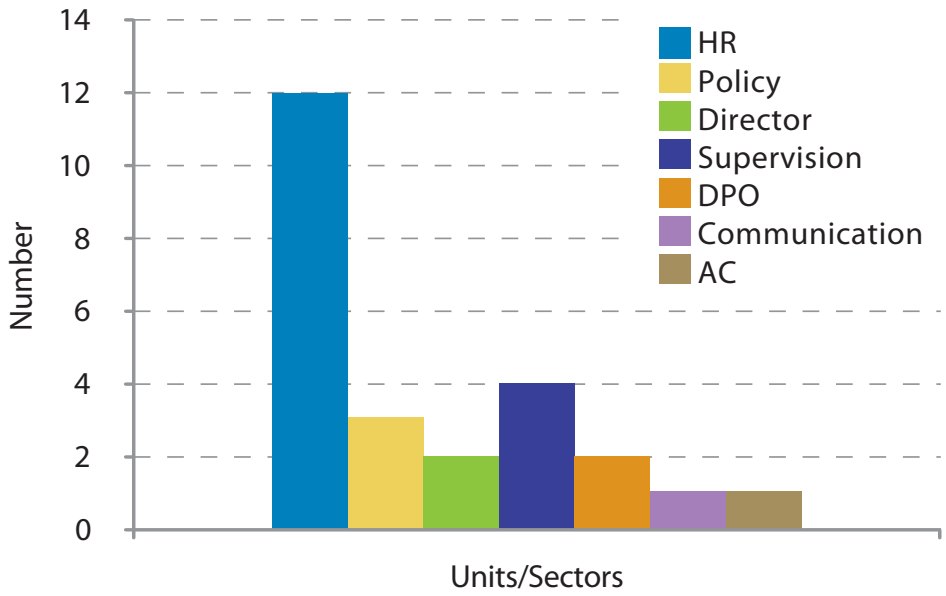
8.2. The Register of processing operations

After the revision of all notifications for processing operations within the EDPS in 2011, the inventory and its implementation were updated in 2012. Consequently, there were 25 new notifications and 2 revisions of existing notifications.



[34] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 14 October 2010

Notifications Article 25 by EDPS Units/Sectors



As a result, 93.02 % of the inventory has been notified and implemented.

The 25 new notifications relating to Article 25 of Regulation 45/2011 were distributed among the EDPS units and sectors as above.

Major efforts by the HR team made it possible that all notifications relating to processing operations were completed. Other units, sectors and functions (such as the Director, DPO and Accounting Correspondent/AC) have fewer individual processing operations to notify, but in total these other controllers were responsible for 52 % of new notifications. The graph above gives a global overview of all processing operations within the institution.

Following EDPS Guidelines, the DPO took care of the notifications submitted to the EDPS under Article 27.2 of Regulation 45/2001. In the event, very few notifications were subject to this provision in 2012.

The DPO's main objective for 2013 is to deal with the 3 missing notifications (one relating to the Case Management System, which will be fully implemented in the course of 2012 and two others from the Staff Committee), in addition to any new processing operations which may arise during the course of the year.

8.3. EDPS 2012 Survey on the status of DPOs

In May 2012, 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 June, the EDPS Director replied to the survey with a complete overview of the status and evolution of the DPO function within the EDPS itself. The information provided relates to the appointment and mandate, training, position and resources of the DPO.

8.4. Information and raising awareness

The DPO places great importance on raising awareness of staff involved in various processing operations and on communication of data protection compliance at the EDPS, both externally and internally.

With regard to **external communication**, the dedicated DPO section on the EDPS website, which offers information about the DPO role and activities, is updated regularly, so that the updated register and all notifications are available for public consultation. In October 2012, the first request for public access to the register was received by the DPO. A reply was sent promptly the following day with a link to the Register on the EDPS website.

In 2012, the DPO took part in the **DPO network meetings** in Helsinki and Frankfurt. These meetings represent a unique opportunity to network, discuss common concerns and share best practices. It has been agreed that the EDPS will host the DPO network meeting in the second half of 2013.

With regard to **internal communication**, the EDPS intranet provides an effective means of communication with staff. The DPO intranet section contains information that is useful to staff members: 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 contains a very detailed list of privacy statements (25 new legal notices) with all relevant information (according to Articles 11 and 12 of Regulation 45/2001) about EDPS processing operations, allowing all members of staff to exercise their rights.

The DPO was also consulted on the possible use of Twitter by the EDPS. In the light of her advice, the Management Board decided in favour of using this new means of communication with stakeholders. The resulting disclaimer on the use of Twitter as an information platform has been published on the EDPS website. [35]

The DPO also raises awareness by regularly presenting *Initiation to Regulation 45/2001* to newcomers, trainees and officials who may not be experts in data protection. The purpose is to familiarise staff members with our data protection mission and values.

[35] See http://www.edps.europa.eu/EDPSWEB/edps/EDPS/

9 MAIN OBJECTIVES FOR 2013

The following objectives have been selected for 2013 within the overall Strategy for 2013-2014. The results will be reported in 2014.

9.1. Supervision and enforcement

- **Ex post prior checks**

When the EDPS was established in 2004, there was a back-log of cases for prior checking relating to processing operations already in place (*ex-post* prior checks). It was decided, therefore, to accept *ex-post* notifications despite the absence of a legal basis for this practice. This phase is now coming to an end, as we consider that EU institutions and bodies have had sufficient time to notify their existing processing operations to us. To this end, the EDPS wrote to the EU institutions and bodies in July 2012 to set a deadline of June 2013 for notifications of all ex-post prior checks. This is expected to give rise to an increase in our workload in the first half of 2013.

- **Guidance and training**

The introduction of the concept of accountability in the data protection framework implies that EU administrations will have to take all necessary measures to ensure compliance and maintain documentation demonstrating that these measures are effective. The EDPS believes that DPOs and DPCs play a significant role in any accountability programme. To support the work of the DPOs and DPCs and to help promote a data protection culture in EU institutions, we will continue to provide guidance and training and encourage close contacts with the DPO network.

- **Closer dialogue with EU institutions**

In the strategic review consultation process our stakeholders underlined the challenge of ensuring the respect of data protection rules and taking into account the constraints of EU administration. Our success will rely on a thorough understanding of data protection requirements by controllers, DPOs and DPCs. As part of Objective 1 of our Strategy 2013-2014 we will maintain our close contact and dialogue with EU institutions to encourage a better understanding of the institutional context and promote a pragmatic and practical application of the regulation. This dialogue could take a number of forms, most notably workshops on a particular theme, meetings or conference calls.

- **General stock taking exercises**

The EDPS intends to launch a new stock taking exercise across all EU institutions and bodies. This is part of a regular exercise whereby we request written feedback on certain indicators of compliance against the respective obligations. The findings of this survey will serve to identify those institutions which lag behind in their compliance programme and to address any identified shortcomings.

- **Visits**

The commitment of management is crucial to the success of ensuring compliance with data protection in the EU administration. We will continue in our efforts to raise awareness at all levels of management and we will make use of our enforcement powers where necessary. We will visit those bodies that fail to communicate with us adequately or demonstrate a clear lack of engagement in complying with the data protection regulation.

- **Inspections**

Inspections are a useful tool that enables us to monitor and ensure the application of the regulation. We intend to further define our inspection policy and to fine-tune the procedure surrounding the inspection process. We will continue to carry out targeted inspections not only in those areas where we have offered guidance but also when we wish to check the status.

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 and integrates data protection in new legislation and sets forth the actions we have designed to achieve this objective. We face the challenge of fulfilling our increasing role in the legislative procedure and extending timely and authoritative advice with increasingly limited resources. In light of this, we have used our inventory of policy issues to select issues of strategic importance that will form the cornerstones of our consultation work for 2013 (the inventory and accompanying note are published on our website).

- **Towards a new legal framework for data protection**

We will give priority to the ongoing review process on a new legal framework for data protection in the EU. We have issued an opinion on the legislative proposals for the framework and will continue to contribute to the debates in the next steps of the legislative procedure where necessary and appropriate.

- **Technological developments and the Digital Agenda, IP rights and Internet**

Technological developments, especially those connected to the internet and the associated policy responses will be another area of our focus in 2013. Subjects range from the plans for a Pan-European framework for electronic identification, authentication and signature, the issue of internet monitoring (such as the enforcement of IP rights and takedown procedures) to cloud computing services. We will also strengthen our technological expertise and engage in research on privacy-enhancing technologies.

- **Further developing the Area of Freedom, Security and Justice**

The AFSJ will remain one of the key policy areas for us to address. Relevant upcoming proposals include the establishment of a European Public Prosecutor's Office to fight against crimes affecting the EU budget and the reform of EUROJUST. In addition, we will continue to follow those initiatives carried over from last year such as the EUROPOL reform and the package on smart borders. We will also closely monitor negotiations with third countries on data protection agreements.

- **Financial sector reforms**

We will continue to follow and scrutinise new proposals for the regulation and supervision of financial markets and actors insofar as they affect the right to privacy and data protection. This is all the more important as a growing number of proposals to harmonise and centrally supervise the financial sector are being put forward.

- **eHealth**

In light of a growing trend to incorporate digital technologies when providing health care services, the establishment of clear rules regarding the use of personal information within that framework is paramount, especially given the sensitive nature of health data. We will follow developments in this area and intervene where appropriate to ensure that data protection principles are respected and enforced.

- **Other initiatives**

We envisage publishing so called *prospective opinions* intended to provide valuable input to the future dissemination of fundamental data protection principles and concerns in other EU policy areas such as competition and trade.

9.3. Cooperation

We will pay particular attention to fulfilling the 2013-2014 Strategy concerning cooperation with other data protection authorities, international organisations and our responsibilities in the field of coordinated supervision.

- **Coordinated supervision**

We will continue in our role in the coordinated supervision of EURODAC, CIS and VIS. In this capacity, we oversaw the establishment of the Supervision Coordination Group of the VIS in November 2012. The second generation Schengen Information System (SIS II) will also be subject to coordinated supervision; its go-live is scheduled for 2013 and preparations will be followed closely as the creation of the new agency for large-scale IT systems only became operational in December 2012. We will also carry out inspections of the central units of these systems where necessary or legally required.

- **Cooperation with data protection authorities**

We will continue to actively contribute to the activities and success of the Article 29 Working Party, ensuring consistency and synergy between it and the EDPS in line with our respective priorities. We will also maintain our good relationships with national DPAs. As rapporteur for some specific dossiers, we will steer and prepare the adoption of WP29 opinions.

- **Data protection in international organisations**

International organisations are often not subject to data protection legislation in their host countries, however, not all of them have their own appropriate rules for data protection in place. The EDPS will therefore continue to reach out to international organisations through an annual workshop which aims to raise awareness and exchange good practice.

9.4. Other fields

- **Information and communication**

In line with our Strategy 2013-2014, the EDPS will continue to raise awareness of data protection within the EU administration, but also in our efforts to inform individuals of their fundamental rights to privacy and data protection. To do this effectively, we will develop our creative communication strategy to garner both public confidence and the commitment of the EU institutions. This will include:

- updating and further developing our website;
- developing new communication tools to make core activities more visible;

- using straightforward language to make technical issues more accessible, together with examples with which the general public can easily identify.

- **Resource management and professionalising the HR function**

In the framework of economic austerity and the need 'to do more with less', the strategy of quality management will be developed to allow the institution to fulfil its tasks in the most efficient way. This will include:

- a specific emphasis on a new training policy, in order to foster professional skills, promote career development and improve performance

- renewed efforts on better planning, performance and monitoring of the spending of financial resources,

- a more strategic approach to human resources management, and

- a total quality management system which will be developed and implemented with clear links between Internal Control Standards, Risk Management and the Common Assessment Framework.

We will also launch a strategic reflection on mid and long-term resource needs, in particular in the context of the future European Data Protection Board.

- **Information technology infrastructure**

Over the course of the year we aim to go-live with our new case management system, to deliver results along the desired timeline, with due regard to the necessary security and data protection safeguards.

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)	Maria ARSENE	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)	Ingrid HVASS. a.i Carine CLAEYS	Ingrid.HVASS@eeas.europa.eu Carine.CLAEYS@eeas.europa.eu
European Ombudsman	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)	Edina TELESSY	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
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	Ignacio Vázquez MOLINÍ	Ignacio.Vazquez-Molini@emcdda.europa.eu

>>>

ORGANISATION	NAME	E-MAIL
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	Spyros.Antoniou@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)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
European Aviation Safety Agency (EASA)	Francesca PAVESI a.i. Frank Manuhutu	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)	Zsófia SZILVÁSSY	Zsofia.Szilvassy@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
European Research Council Executive Agency (ERCEA)	Nadine KOLLOCZEK	Nadine.Kolloczek@ec.europa.eu
Research Executive Agency (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu

>>>

ORGANISATION	NAME	E-MAIL
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 a.i. Francesca LOMBARDO	roberta.maggio@eit.europa.eu
European Defence Agency (EDA)	Alain-Pierre LOUIS	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

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

E-mail system – ERA

Opinion of 6 December 2012 on the notification for prior checking from the Data Protection Officer of the European Railway Agency (ERA) regarding ERA's e-mail system and back-end e-mail system (Cases 2012-136 and 137)

Internet system – ERA

Opinion of 6 December 2012 on the notification for prior checking from the Data Protection Officer of the European Railway Agency (ERA) regarding the use of ERA's Internet system (Case 2012-0135)

In-house scientific expertise database-EFSA

Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Food Safety Authority ("EFSA") regarding the "EFSA in-house scientific expertise database" (Case 2011-0882)

Internal mobility procedure – ERCEA

Opinion of 3 December 2012 on a notification for prior checking received from the Data Protection Officer of the European Research Council Executive Agency (ERCEA) regarding ERCEA's internal mobility procedure for Temporary and Contractual Agents (Case 2012-0870)

Clinical study in the frame of the research project PROTECT WP4 – EMA

Opinion of 29 November 2012 on a notification for prior checking received from the Data Protection Officer of the European Medicines Agency related to the "clinical study in the frame of the research project PROTECT WP4", (Case 2012-0704)

Selection procedure for the position of a member of the Management Board – EMA

Opinion of 26 November 2012 on the notification for prior checking from the Data Protection Officer of the European Commission concerning the selection procedure for the position of a member of the Management Board of the European Medicines Agency (EMA) and for the position of a member of the following scientific committees of EMA: Committee for Advance Therapies, Committee for Orphan Medicinal Products, Paediatric Committee and Pharmacovigilance Risk Assessment Committee (Case 2011-1166)

Télétravail – Conseil de l'Union européenne

Avis du 23 novembre 2012 sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Secrétariat Général du Conseil à propos du dossier «télétravail» (Dossier 2012-0661)

Anti-harassment procedures – EMSA

Opinion of 23 November 2012 on the notification for prior checking concerning anti-harassment procedures at EMSA (Case 2012-0302)

Administrative enquiries – FRA

Opinion of 23 November 2012 on the notification for prior checking concerning administrative enquiries at the Fundamental Rights Agency (FRA) (Case 2012-0683)

Invalidity Committee – Eurofoud

Opinion of 20 November 2012 on the notification for prior checking concerning Invalidity Committee at Eurofound (Case 2011-0643)

Attestation procedure – Cedefop

Opinion of 19 November 2012 on the notification for prior checking from the Data Protection Officer of the Cedefop concerning Attestation procedure (Case 2012-0706)

Internet monitoring – CEDEFOP

Opinion of 15 November 2012 on a notification for prior checking received from the Data Protection Officer of the European Centre for the Development of Vocational Training (CEDEFOP) related to Internet monitoring (processing of data in connection with a Proxy system) (Case 2011-1069)

Staff evaluation – EASA

Opinion of 22 October 2012 on the notification for prior checking concerning staff evaluation procedures at EASA (Case 2011-1113)

Probation, Annual Appraisal, Promotion – F4E

Opinion of 16 October 2012 on the notifications for prior checking from the Data Protection Officer of

the Fusion for Energy concerning Probation, Annual Appraisal, Promotion, Regrading and Reclassification (Cases 2012-404, 405, 406, 407 and 408)

Assistance, Human Factors experts, Investigation of railway accidents – ERA

Opinion of 10 October 2012 on the notification for prior checking from the Data Protection Officer of the European Railway Agency concerning the "Call for applications for inclusion on a list of Human Factors experts to assist the National Investigation Body in some Member States in the investigation of railway accidents" (Case 2012-0635)

"Instance spécialisée en matière d'irrégularités financières" – Council of the European Union

Opinion of 26 September 2012 on the notification for prior checking concerning «Instance spécialisée en matière d'irrégularités financières» – Council of the European Union (Case 2012-0533)

Health data – EACEA

Opinion of 12 September 2012 on the notification for prior checking concerning processing of personal data related to health at EACEA (Case 2012-0537)

Entrance permission and access control for physical protection (ZES+ZKS) at JRC-ITU in Karlsruhe – European Commission

Opinion of 24 July 2012 on the notification for prior checking concerning Entrance permission and access control for physical protection (ZES+ZKS) at JRC-ITU in Karlsruhe, European Commission (Case 2008-0726)

Annual Declaration of Interest – ECDC (European Centre for Disease Prevention and Control)

Opinion of 19 July 2012 on a notification for Prior Checking received from the Data Protection Officer of the European Centre for Disease Prevention and Control regarding Annual Declaration of Interests (Case 2010-0914)

Staff appraisal – CdT

Opinion of 19 July 2012 on the notification for prior checking received from the Data Protection Officer of the Translation Centre concerning staff appraisal (Case 2012-475)

"Désignation du 3e/2e médecin dans la commission d'invalidité et commission médicale" – Court of Justice

Opinion of 18 July 2012 on the notification for prior checking concerning «Désignation du 3ème/2ème médecin dans la commission d'invalidité et commission médicale» – Court of Justice (Case 2011-0775)

Complaints under Article 90a of the Staff Regulations – OLAF

Opinion of 16 July 2012 on the notification for prior checking from the Data Protection Officer of the European Anti-Fraud Office (OLAF) regarding the processing of personal data in relation to complaints under Article 90a of the Staff Regulations (Case 2012-0274)

Disciplinary procedures and administrative enquiries – CdT

Opinion of 06 July 2012 on the notification for prior checking concerning Disciplinary procedures and administrative enquiries, Translation Centre (Case 2011-0916)

Inter-institutional exchanges of staff of the language services

Joint Opinion of 5 July 2012 on a notification for Prior Checking received from the Data Protection Officers of the European Commission, the Council, the European Parliament, the European Central Bank, the Translation Centre for the Bodies of the European Union, the European Economic and Social Committee, the Committee of the Regions and the European Court of Auditors regarding the inter-institutional exchanges of staff of the language services of the EU institutions and bodies (Joint cases 2011-0560 and 2011-1029)

Selection and appointment of two Stakeholder Groups – EIOPA

Opinion of 3 July 2012 on the notification for prior checking the selection and appointment of the two Stakeholder Groups at the European Insurance and Occupational Pensions Authority (EIOPA) (case 2012-0264)

"Gestion du Bureau Véhicules de Service" – Council of the European Union

Opinion of 27 June 2012 on the notification for prior checking concerning "Gestion du Bureau Véhicules de Service" – Council of the European Union (Case 2012-0157)

Certification – CdT

Opinion of 11 June 2012 on the notification for prior checking concerning certification procedure, Translation Centre (Case 2011-1156)

Promotion, Career Advancement and Assessment of the Senior and Middle Management – Cedefop

Opinion 11 June 2012 on the notification for prior checking concerning Promotion, Career Advancement, as well as Assessment of the Senior and Middle Management, Cedefop (Cases 2012-009 and 2012-010)

Probation, Career Development Review and Reclassification – EAHC

Opinion of 11 June 2012 on the notification for prior checking concerning Probation, Career Development Review and Reclassification, Executive Agency for Health and Consumers (Cases 2010-828 and 2012-149)

Probation – ERA

Opinion of 14 June 2012 on the notifications for prior checking concerning Probation, CDR, Reclassification, Evaluation of the Ability to Work in a Third Language, Use of Performance Indicators in the CDR of the FIA, as well as Renewal of Contract of Employment of the European Railway Agency statutory staff, (Cases 2011-960, 2011-961, 2011-962, 2012-087 and 2012-138)

Health data – F4E

Letter of 7 June 2012 on the notifications for prior checking concerning health data processing at F4E (Cases 2011-1088, 2011-1089, 2011-1090, 2011-1091)

Recording of the telephone line

Opinion of 7 June 2012 on the notification for prior checking concerning the 'Recording of the telephone line reserved for calls to the dispatch centre for technical services used in the European Commission buildings in Luxembourg (12 or 32220)' (Case 2011¬ – 0986)

eRecruitment – EMCDDA

Opinion of 31 May 2012 on the notification for prior checking on e-recruitment procedures at EMCDDA (Case 2012-0290)

Staff Appraisal, Probation and Reclassification – FRONTEX

Opinion of 30 May 2012 on the notification for prior checking on Staff Appraisal, Probation and Reclassification, FRONTEX (Case 2011-969)

Annual Appraisal – EACI

Opinion of 29 May 2012 on notifications for prior checking on Annual Appraisal, Reclassification, Probation and Evaluation of the Ability to Work in a Third Language, Executive Agency for Competitiveness and Innovation (Cases 2011-998, 2011-999 and 2011-1000)

Recording of the telephone line – EC

Opinion of 24 May 2012 on the notification for prior checking concerning the 'Recording of the telephone line used for security guard service reports and calls concerning actions connected with the system for controlling access to Commission buildings (Brussels)', European Commission (Case 2011-0987)

Safe Mission Data system – EP

Opinion of 24 May 2012 on a notification for Prior Checking concerning the "Safe Mission Data" system, European Parliament (Case 2012-0105)

Read More

Vacances d'emploi hors encadrement – European Commission

Opinion of 22 May 2012 on the notification for prior checking concerning «Vacances d'emploi hors encadrement» – European Commission (Case 2012-0276)

Register of telephone calls – EIB

Opinion of 15 May 2012 on the notification for prior checking concerning the case 'Register of tele-

phone calls (mobile telephony)', European Investment Bank (Case 2009-0704)

Studentships scheme – F4E

EDPS opinion of 11 May 2012 on the notification for prior-checking concerning selection procedure for the Fusion for Energy (F4E) studentships scheme and management of the scheme (Case 2012-246)

Grant award and management procedures – EACEA

Opinion of 11 May 2012 on the notification for prior checking concerning grant award and management procedures, Education Audiovisual and Culture Executive Agency (Case 2011-1083)

Processing of personal data by the Ethics and Compliance Committee – EIB

Opinion of 11 April 2012 on the notification for prior checking concerning processing of personal data by the Ethics and Compliance Committee of the European Investment Bank (Case 2011-1141)

Accreditation of journalists to the European Parliament

Opinion of 3 April 2012 on the notification for prior checking concerning the accreditation of journalists to the European Parliament (Case 2011-0991)

Monitoring and Assessment of Auxiliary Conference Interpreters – EC

Opinion of 29 March 2012 on the notification for prior checking concerning Continuous Quality Monitoring and Assessment of Auxiliary Conference Interpreters in DG Interpretation, European Commission (case 2010-912)

Annual Appraisal and Reclassification of Temporary Agents – ENISA

Opinion of 27 March 2012 on the notification for prior checking concerning Annual Appraisal and Reclassification of Temporary Agents, European Network and Information Society Agency (Cases 2010-936 and 2010-937)

Promotion and Reclassification – EFSA

Opinion of 26 March 2012 on the notification for prior checking on Promotion and Reclassification, European Food Safety Authority (case 2012-0079)

Call for expression of interest for selection of experts – EACEA

Opinion of 22 March 2012 on the notification for prior checking concerning call for expression of interest for selection of experts (Case 2012-0007)

Monitoring of external experts' work – EACEA

Opinion of 22 March 2012 on a notification for prior checking on the monitoring of external experts' work (Case 2012-0008)

Performance Appraisal – FRA

Opinion of 21 March 2012 on the notification for prior checking on Performance Appraisal, Probation, Career Advancement, Reclassification, as well as Appraisal and Probation of the Director, European Union Agency for Fundamental Rights (Cases 2011-938, 2011-954, 2011-1076 and 2011-1077)

Organisation of meetings and meals of the Meetings of Heads of States or Governments – Council

Opinion of 16 March 2012 on a notification for prior checking regarding the "Organisation of meetings and meals of the Meetings of Heads of States or Governments, of Summits or Official Meetings with Third Countries and of the Council of the E.U and other Meetings at ministerial level or above" (Case 2011-0933)

Regulations requiring asset freezing

Opinion of 22 February 2012 on a notification for Prior Checking regarding the Processing of personal data in connection with regulations requiring asset freezing as CFSP related restrictive measures, European Commission (Case 2010-0426)

Read More

Holiday Camps – Council

Opinion of 22 February 2012 on the notification of a prior check on the 'Holiday Camps' case, Council of the European Union (Case 2011-0950)

Teleworking – CoR

Opinion of 13 February 2012 on the notification for prior-checking concerning the 'teleworking' case, Committee of the Regions (Case 2011-1133)

Probationary period of Heads of Unit/newly appointed Directors – ECA

Opinion of 13 February 2012 on the notification for prior checking concerning the 'probationary period of Heads of Unit/newly appointed Directors' procedures case, European Court of Auditors (Case 2011-0988)

Staff Evaluation Procedures – EACEA

Opinion of 6 February 2012 on notifications for prior checking concerning career development review, probation and reclassification at the Education, Audiovisual and Culture Executive Agency (joint cases 2010-589, 2011-1071 and 2011-1072)

Staff Evaluation Procedures – CFCA

Opinion of 6 February 2012 on the notification for prior checking concerning Staff Appraisal, Probationary Procedure for contract agents and Reclassification of temporary agents at the Community Fisheries Control Agency (CFCA)(Case 2011-0952)

Investigative procedures – OLAF

Opinion of 3 February 2012 on the notifications for prior checking regarding new OLAF investigative procedures (internal investigations, external investigations, dismissed cases and incoming information of no investigative interest, coordination cases and implementation of OLAF recommendations), European Anti-Fraud Office (OLAF) (Cases 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132)

Administrative inquiries and disciplinary proceedigs – CPVO

Letter of 3 February 2012 concerning the notification for prior checking on the processing of administrative inquiries and disciplinary proceedings at the Community Plant Variety Office (CPVO) (Case 2011-1128)

Establishment of probationers/Management of agents' probationary reports – CoR

Opinion of 26 January 2012 on a notification for prior-checking concerning the case 'Establishment of probationers/Management of agents' probationary reports', Committee of the Regions (Case 2011-1118)

Probationary period and certification – EMCDDA

Opinion of 08 March 2012 on the notifications for prior checking concerning staff recruitment procedures at IMI (Cases 2011-0822 and 2011-1080)

Promotion procedures – Council of the European Union

Letter of 17 February 2012 on the notification for prior checking concerning probationary period and certification procedures at EMCDDA (Case 2011-1161)

Staff recruitment – IMI

Opinion of 13 February 2012 on the notification for prior checking concerning staff recruitment procedures at IMI (Case 2011-0872)

Staff recruitment and appraisal – CleanSky

Opinion of 13 February 2012 on the notification for prior checking concerning staff recruitment and appraisal procedures at CleanSky (Case 2011-0839)

Staff recruitment – Artemis JU

Opinion of 27 January 2012 on the notification for prior checking concerning staff recruitment procedures at Artemis Joint Undertaking (Case 2011-0831)

Selection of confidential counsellors and the informal procedures for cases of harassment – CPVO

Opinion of 23 January 2012 on the notification for prior checking concerning the selection of confidential counsellors and the informal procedures for cases of harassment at the Community Plant Variety Office (CPVO) (Case 2011-1073)

Public procurement and grant award procedures – CEDEFOP

Opinion of 19 January 2012 on the notification for prior checking concerning public procurement and grant award procedures at the European Centre for the Development of Vocational Training (CEDEFOP) (Case 2011-0542)

Staff Evaluation Procedures – FCH JU

Opinion of 16 January 2012 on the notification for prior checking concerning annual appraisal and probation at the Fuel Cells Hydrogen Joint Undertaking (Case 2011-835)

Procurement procedures – Community Fisheries Control Agency

Opinion of 13 January 2012 on the notifications for prior checking concerning the Call for expression of interest No. CFCA/2010/CEI/01 and subsequent contracts at the the Community Fisheries Control Agency (Case 2011-1001)

"Sous-traitance partielle de la Caisse Maladie" – EIB

Letter of 10 January 2012 on the modified notification for prior checking on the «Sous-traitance partielle de la Caisse Maladie» at the European Investment Bank (Case 2011-1039)

Staff evaluation procedures – EU-OSHA

Joint Opinion of 9 January 2012 on the notifications for prior checking regarding staff evaluation procedures at the European Agency for Safety and Health at Work (EU-OSHA) (Cases 2011-957, 2011-958, 2011-959)

List of non prior checks 2012

Professional Profile Map – ECDC

Letter of 20 December 2012 regarding prior-checking notification on the processing operations related to the Professional Profile Map at ECDC (Case 2012-0900)

Statutory staff – ERCEA

Letter of 20 December 2012 regarding prior-checking notification on the processing operations related to the termination of the service of ERCEA statutory staff (Case 2012-0898)

Training activities – ERCEA

Letter of 19 December 2012 regarding a notification for a prior-checking on "Management of training requests and training activities for ERCEA staff" (Case 2012-0915)

Telephone Use – ETF

Answer of 11 December 2012 regarding personal data processing operations relating to the Telephone Use at the ETF for prior checking (Case 2012-0917)

Study on staff satisfaction – EACI

Answer of 9 October 2012 on the notification on the processing operations relating to "Study on staff satisfaction at the EACI" (Case 2012-0527)

Processing operations within the MATRIX application – FRA

Answer of 12 September 2012 on the notification for prior-checking regarding the processing operations within the MATRIX application at Fundamental Right Agency (FRA) (Case 2012 – 0090)

Search Facility – OLAF

Opinion of 10 August 2012 on the notification for prior checking from the Data Protection Officer of the European Anti-Fraud Office (OLAF) regarding the processing of personal data in relation to the Search Facility

Flexitime – FRA

Answer of 13 April 2012 on the notification for prior checking regarding the processing operations on flexitime at Fundamental Right Agency (FRA) (Case 2012-0089)

European Union Transaction Log (EUTL) – European Commission

Answer of 13 April 2012 on the notification for prior checking regarding the processing operations on European Union Transaction Log (EUTL) at the European Commission (Case 2011-1153)

External activity – European Ombudsman

Answer of 12 January 2012 on the notification for prior checking regarding the processing operations concerning external activities of EO personnel (Case 2012-0005)

Computer based learning modules – Council

Answer of 10 January 2012 on the notification for prior checking regarding the processing operations on Security Awareness Computer-based Learning Modules at the Council of the European Union (Case 2011-1058)

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

Opinions on legislative proposals

Clinical trials on medicinal products

Opinion of 19 December 2012 on the Commission proposal for a Regulation on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC

Statute and funding of European political parties

Opinion of 13 December 2012 the European Data Protection Supervisor on the Proposal for a Regulation on the statute and funding of European political parties and European political foundations

European Voluntary Humanitarian Aid Corps

Opinion of 23 November 2012 on the Proposal for a Regulation establishing the European Voluntary Humanitarian Aid Corps

Insurance mediation, UCITS and key information documents for investment products

Opinion of 23 November 2012 on proposals for a Directive on insurance mediation, a Directive amending certain provisions of Directive 2009/65/EC on the coordination of laws, regulations and administrative sanctions relating to undertakings for collective investment in transferable securities and a Regulation on key information documents for investment products

Cloud Computing in Europe

Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"

Deposit of the historical archives of the institutions at the European University Institute in Florence

Opinion of 10 October 2012 on the Commission Proposal for a Council Regulation amending Regulation (EEC/Euratom) No 354/83, as regards the deposit of the historical archives of the institutions at the European University Institute in Florence

Financing, management and monitoring of the common agricultural policy (transparency, post-Schecke)

Opinion of 9 October 2012 on the Amendment to the Commission proposal COM(2011) 628 final/2 for a Regulation of the European Parliament and of the Council on the financing, management and monitoring of the common agricultural policy

Electronic Trust Services

Opinion of 27 September 2012 on the Commission proposal for a Regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation)

Establishment of 'EURODAC' for the comparison of fingerprints

Opinion of 5 September 2012 on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…]

Posting of workers in the framework of the provision of services

Opinion of 19 July 2012 on the Commission Proposal for a Directive of the European Parliament and of the Council on the enforcement of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services and on the Commission Proposal for a Council Regulation on the exercise of the right to take collective action within the context of the freedom of establishment and the freedom to provide services

European Strategy for a Better Internet for Children

Opinion of 17 July 2012 on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "European Strategy for a Better Internet for Children"

Improving securities settlement in the European Union

Opinion of 9 July 2012 on the Commission proposal for a Regulation of the European Parliament and of the Council on improving securities settlement in

the European Union and on central securities depositories (CSDs) and amending Directive 98/26/EC

Second generation Schengen Information System (SIS II)

Opinion of 9 July 2012 on the proposal for a Council Regulation on migration from the Schengen Information System (SIS) to the second generation Schengen Information System (SIS II) (recast)

Simplifying the transfer of motor vehicles registered in another Member State

Opinion of 9 July 2012 on the proposal for a Regulation of the European Parliament and of the Council on simplifying the transfer of motor vehicles registered in another Member State within the Single Market

European Cybercrime Center

Opinion of 29 June 2012 on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre

European Venture capital funds

Opinion of 14 June 2012 on the proposals for a Regulation on European Venture capital funds and for a Regulation on European Social entrepreneurship funds

Smart metering systems

Opinion of 8 June 2012 on the Commission Recommendation on preparations for the roll-out of smart metering systems

Union Registry for the trading period commencing on 1 January 2013

Opinion of 11 May 2012 on the Commission Regulation establishing a Union Registry for the trading period commencing on 1 January 2013, and subsequent trading periods, of the Union emissions trading scheme

Anti-Counterfeiting Trade Agreement (ACTA)

Opinion of 24 April 2012 on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America

Open-Data Package

Opinion of 18 April 2012 on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI)

Statutory audits

Opinion of 13 April 2012 on the Commission proposals for a Directive amending Directive 2006/43/EC on statutory audit of annual accounts and consolidated accounts, and for a Regulation on specific requirements regarding statutory audit of public-interest entities

EU-Canada Agreement on supply chain security

Opinion of 13 April 2012 on the Proposal for a Council decision on the conclusion of the Agreement between the European Union and Canada with respect to matters related to supply chain security

Cross-border threats to health

Opinion of 28 March 2012 on the proposal for a decision of the European Parliament and of the Council on serious cross-border threats to health

Review of the Professional Qualifications Directive

Opinion of 8 March 2012 on the Commission proposal for a Directive of the European Parliament and of the Council amending Directive 2005/36/EC on the recognition of professional qualifications and Regulation [...] on administrative cooperation through the Internal Market Information System

Data protection reform package

Opinion of 7 March on the data protection reform package

Driving licences including functionalities of a driver card

Opinion of 17 February 2012 on the proposal for a Directive of the European Parliament and of the Council amending Directive 2006/126/EC of the European Parliament and of the Council as regards

driving licences which include the functionalities of a driver card

Credit rating agencies

Opinion of 10 February 2012 on the Commission proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1060/2009 on credit rating agencies

Insider dealing and market manipulation

Opinion of 10 February 2012 on the Commission proposals for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, and for a Directive of the European Parliament and of the Council on criminal sanctions for insider dealing and market manipulation

Markets in financial instruments

Opinion of 10 February 2012 on the Commission proposals for a Directive of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council (Recast), and for a Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation on OTC derivatives, central counterparties and trade repositories

Access to the activity of credit institutions

Opinion of 10 February 2012 on the Commission proposals for a Directive on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and for a Regulation on prudential requirements for credit institutions and investment firms

EU-US Joint Customs Cooperation

Opinion of 9 February 2012 on the Proposal for a Council decision on a Union position within the EU-US Joint Customs Cooperation Committee regarding mutual recognition of the Authorised Economic Operator Programme of the European Union and the Customs-Trade Partnership Against Terrorism Program of the United States

Administrative Cooperation in the field of Excise Duties

Opinion of 27 January 2012 on the Proposal for a Council Regulation on Administrative Cooperation in the field of Excise Duties

Alternative and Online Dispute Resolution for consumer disputes

Opinion of 12 January 2012 on the legislative Proposals on Alternative and Online Dispute Resolution for consumer disputes

Formal comments on legislative proposals

Interoperable EU-wide eCall

Letter of 19 December 2012 on Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall (C(2012)8509 final)

Consultation on self-regulation

Letter of 19 December 2012 regarding Commission Consultation on self-regulation

Code of conduct for archives

Letter of 3 December 2012 to Ms Day, Secretary General of the European Commission concerning the plans of the European Board of National Archivists (EBNA) and the European Archives Group (EAG) to prepare a code of conduct for the archives sector to address the application of data protection requirements, taking into account the specificities of the sector.

Protection of personal data in New Zealand

Letter of 9 November 2012 to Ms Françoise Le Bail, Director-General for DG Justice concerning the draft Commission Implementing Decision on the adequate protection of personal data in New Zealand pursuant to Directive 95/46/EC

Open internet

EDPS comments of 15 October 2012 on DG Connect's public consultation on specific aspects of transparency, traffic management and switching in an open internet

Improving network and information security (NIS) in the EU

EDPS comments of 10 October 2012 on DG Connect's public consultation on improving network and information security (NIS) in the EU

Collective management of copyright

Letter of 9 October 2012 to Mr Michel BARNIER, Commissioner for Internal Market and Services concerning proposed Directive on Collective management of copyright

Illegal content hosted by online intermediaries

EDPS comments of 13 September 2012 on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries

European Consumer Agenda – Boosting confidence and growth

EDPS Comments of 16 July 2012 on the Commission Communication – A European Consumer Agenda – Boosting confidence and growth

EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016

EDPS comments of 10 July 2012 on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016"

Proposal for directive on freezing and confiscating proceeds of crime

Letter of 18 June 2012 to Ms Cecilia Malmström, European Commissioner for Home Affairs concerning proposal for directive on freezing and confiscating proceeds of crime

Special Committee on Organised Crime, Corruption and Money Laundering (CRIM)

Letter of 7 June 2012 to Ms Sonia Alfano, MEP, concerning EDPS involvement in Special Committee on Organised Crime, Corruption and Money Laundering (CRIM)

European market for card, internet and mobile payments

Letter of 11 April 2012 concerning Commission's Green Paper "Towards an integrated European market for card, internet and mobile payments"

European Border Surveillance System (EUROSUR)

EDPS comments of 8 February 2012 on the Commission proposal for establishing the European Border Surveillance System (EUROSUR)

Responsible Business

Letter of 10 January 2012 concerning "Responsible Business" package adopted by the Commission on 25 October 2011

Annex G — Speeches by the Supervisor and Assistant Supervisor in 2012

The Supervisor and the Assistant Supervisor continued to invest substantial time and effort in 2012 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

8 February	Supervisor, S&D conference on Improved Schengen Governance (Brussels) (*)
6 March	Supervisor, Conference on Genetic Discrimination (Brussels)
15 March	Supervisor, Conference on EU administrative law (Brussels)
27 March	Supervisor, European Internet Foundation on Cloud Computing (Brussels)
28 March	Supervisor, Privacy Platform on the proposed Data Protection Regulation (Brussels)
25 April	Assistant Supervisor, IMCO Committee on growth & mobility (Brussels) (*)
26 April	Assistant Supervisor, LIBE Committee on ACTA (Brussels) (*)
16 May	Assistant Supervisor, LIBE Committee workshop on ACTA (Brussels) (*)
29 May	Supervisor, LIBE workshop on the proposed Data Protection Regulation (Brussels) (*)
20 June	Supervisor and Assistant Supervisor, LIBE Committee on Annual Report 2011 (Brussels)
26 June	Supervisor, Greens' conference on "Emerging e-Fortress Europe" (Brussels) (*)
28 June	Supervisor, Greens/EFA hearing on Data Protection Reform (Brussels) (*)
10 October	Supervisor, Inter-parliamentary hearing on Data Protection Reform (Brussels) (*)
11 October	Supervisor, LIBE Committee on the EURODAC Regulation (Brussels) (*)

Council

24 January	Supervisor, Polish Permanent Representation on Data Protection Day (Brussels)
2 February	Supervisor, Danish Presidency conference "One Europe – One Market" (Copenhagen) (*)
14 March	Supervisor, WP on Data Protection and Information Exchange (Brussels)
4 October	Supervisor, International Conference on Cyberspace (Budapest)

European Commission

25 January	Supervisor and Assistant Supervisor, DPO and DPCs on Data Protection Day (Brussels)
19 March	Supervisor, EU Conference on Privacy and Data Protection (Washington DC) (*)
30 May	Supervisor, European Archives Group on Data Protection Reform (Copenhagen)
21 June	Supervisor, Digital Assembly on Data Protection Reform (Brussels)
24 September	Supervisor, EU Anti-Human Trafficking Coordinator seminar (Brussels)

Other EU institutions and bodies

10 May	Supervisor, Fundamental Rights Agency on Data Protection Reform (Vienna) (*)

16 May	Assistant Supervisor, ERA seminar on Cybercrime Centre in Europol (Brussels) (*)
20 September	Supervisor and Assistant Supervisor, ERA conference on new DP Regulation (Trier)
19 October	Assistant Supervisor, Heads of Agencies (Stockholm) (*)
5 November	Supervisor and Assistant Supervisor, ERA conference on new DP Directive (Trier)
8 November	Supervisor and Assistant Supervisor, Workshop International Organisations (Brussels)

International Conferences

27 January	Supervisor, Conference on Computers, Privacy and Data Protection (Brussels)
9 March	Supervisor, IAPP Global Privacy Summit (Brussels)
3 May	Supervisor and Assistant Supervisor, European Data Protection Authorities (Brussels)
7 May	Supervisor, European Data Protection Day (Berlin)
9 October	Supervisor, Amsterdam Privacy Conference (Amsterdam)
22 October	Supervisor, Public Voice conference (Punta del Este, Uruguay)
23 October	Supervisor and Assistant Supervisor, Privacy and Data Protection Commissioners (Punta del Este, Uruguay)
15 November	Supervisor, IAPP Europe Data Protection Congress (Brussels)
3 December	Supervisor, IAPP Europe Knowledge Net conference (Brussels) (*)
4 December	Supervisor, Data Protection & Privacy Conference (Brussels) (*)

Other events

18 January	Supervisor, 5th Annual Conference on Processing of Personal Data (Paris) (*)
20 January	Supervisor, American Chamber of Commerce on Digital Economy (Brussels)
26 January	Supervisor, European Academy on Data Protection Reform (Berlin)
17 February	Supervisor, European Biometrics Association (Brussels)
22 February	Supervisor, Workshop on Accountability (Brussels)
24 February	Supervisor, Conference on Emerging Challenges in Privacy Law (Melbourne) (* and **)
5 March	Supervisor, European Affairs Platform (Brussels)
8 March	Supervisor, Westminster e-Forum on Data Protection Reform (London)
15 March	Supervisor, Forum on Binding Corporate Rules (Amsterdam)
20 March	Supervisor, C-PET on Data Protection Reform (Washington DC)
21 March	Assistant Supervisor, Conference on Cloud Computing (Brussels) (*)
26 March	Supervisor, European Voice on Data Protection Reform (Brussels)
27 March	Supervisor, American Chamber of Commerce in France (Paris) (*)
29 March	Supervisor, Dutch Privacy Association (Utrecht)
12 April	Supervisor, Tech America on Data Protection Reform (Brussels)
16 April	Supervisor, Workshop on National Human Rights Institutes (Leuven)

20 April	Supervisor and Assistant Supervisor, Privacy Seminar (Cambridge)
24 April	Supervisor, EU-US Forum on Economic Law (Brussels)
26 April	Supervisor, Berkeley Law Forum (Palo Alto, US) (*)
27 April	Supervisor, Future of Privacy Forum (Mountain View, US)
22 May	Supervisor, Privacy Law Forum (Frankfurt)
31 May	Supervisor, Workshop on Accountability (Brussels)
6 June	Supervisor, ISMS Forum on Data Protection Reform (Madrid)
8 June	Supervisor, Digital Europe on Data Protection Reform (Brussels)
8 June	Assistant Supervisor, Columbia Institute for Tele-Information (New York) (*)
11 June	Supervisor, Reuters Summit on Data Protection Reform (London)
12 June	Supervisor, Data Protection and Freedom of Expression (Oxford) (*)
15 June	Supervisor, Data Protection Law conference (Fribourg)
18 June	Supervisor, DuD 2012 on Data Protection Reform (Berlin) (*)
19 June	Supervisor, Digital E-Forum on Data Protection Reform (Luxembourg)
20 June	Supervisor, Eurosmart on Data Protection Reform (Brussels)
21 June	Supervisor, Time.Lex (Brussels)
21 June	Assistant Supervisor, Am Cham Italy and US mission (Rome) (*)
25 June	Supervisor, Economic Council on Data Protection Reform (Brussels)
26 June	Supervisor, Cabinet DN on Data Protection Reform (Brussels)
27 June	Supervisor, Biometrics Institute (London)
12 July	Supervisor, Microsoft on Data Protection Reform (Brussels)
12 September	Supervisor, Freedom – Not Fear (Brussels)
19 September	Supervisor, World Smart Week on Data Protection Reform (Nice)
3 October	Supervisor, CEPS on e-monitoring (Brussels)
16 October	Supervisor, GSMA-ETNO Seminar on e-Privacy (Brussels) (*)
7 November	Supervisor, Swiss Re on Global Data Protection (Zürich)
13 November	Supervisor, Internet of Things Europe (Brussels)
14 November	Supervisor, E-Commerce Europe (Brussels)
26 November	Supervisor, ECTA on Data Protection Reform (Brussels)
28 November	Supervisor, Eurocommerce on Data Protection Reform (Brussels)
30 November	Supervisor, European Council of Medical Orders (Brussels)

(*) Text available on the EDPS website

(**) Video 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*	Pierre VERNHES (*) *Legal Adviser*
Jaroslaw LOTARSKI (*) *Head of Complaints*	Maria Verónica PEREZ ASINARI *Head of Administrative Consultations*
Delphine HAROU *Head of Prior Checks*	Athena BOURKA (*) *Seconded National Expert*
Raffaele DI GIOVANNI BEZZI *Legal Officer*	Elisabeth DUHR (*) *Seconded National Expert*
Daniela GUADAGNO *Legal Officer/Seconded National Expert*	Ute KALLENBERGER *Legal Officer*
Xanthi KAPSOSIDERI *Legal Officer*	Luisa PALLA *Supervision and Enforcement Assistant*
Antje PRISKER *Legal Office*	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*	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*	Katarzyna CUADRAT-GRZYBOWSKA (*) *Legal Officer*
Priscilla DE LOCHT *Legal Officer*	Amanda JOYCE *Policy and Consultation Assistant*
Elise LATIFY *Legal Officer*	Per JOHANSSON *Legal Officer*
Owe LANGFELDT (*) *Legal Officer / Interim*	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*	Bart DE SCHUITENEER *Technology Officer LISO*
Luis VELASCO (*) Technology Officer	

• Operations, Planning and Support

Andrea BEACH *Head of Sector*	Marta CORDOBA-HERNANDEZ *Administrative Assistant*
Kim DAUPHIN *Administrative Assistant/Interim*	Milan KUTRA *Administrative Assistant*
Kim Thien LÊ *Administrative Assistant*	Ewa THOMSON *Administrative Assistant*

• Information and Communication

Olivier ROSSIGNOL *Head of Sector*	Parminder MUDHAR *Information and Communication Specialist*
Agnieszka NYKA *Information and Communication Specialist*	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*
Isabelle DELATTRE (*) *Finance and Accounting Assistant*	Anne LEVÊCQUE *Human Resources Assistant* *& official managing leave*
Vittorio MASTROJENI *Human Resources Officer*	Julia MALDONADO MOLERO (*) *Administration Assistant/Interim*
Daniela OTTAVI *Finance and Procurement Officer*	Aida PASCU *Administration Assistant* *LSO*
Sylvie PICARD *Data Protection Officer* *ICC*	*Anne-Françoise REYNDERS* *Human Resources Assistant* *& Training coordinator*

(*) Staff members who left the EDPS in the course of 2012

The European Data Protection Supervisor

Annual Report 2012

Luxembourg: Publications Office of the European Union

2013 — 125 pp. — 21 × 29.7 cm

ISBN 978-92-95076-78-5
doi:10.2804/52280

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- via EU Bookshop (http://bookshop.europa.eu);
- at the European Commission's representations or delegations. You can obtain their contact details on the Internet (http://ec.europa.eu) or by sending a fax to +352 2929-42758.

Priced publications:

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

Priced subscriptions (e.g. annual series of the Official Journal of the European Union and reports of cases before the Court of Justice of the European Union):

- via one of the sales agents of the Publications Office of the European Union (http://publications.europa.eu/others/agents/index_en.htm).

EUROPEAN DATA
PROTECTION SUPERVISOR

QT-AA-13-001-EN-C

The European guardian of data protection

www.edps.europa.eu

@EU_EDPS

ISBN 978-92-95076-78-5

Publications Office