ISSN 1830-5474

Annual Report

2011

European Data Protection Supervisor

Annual Report

2011

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, 2012

ISBN 978-92-95073-28-9
doi:10.2804/35928

Printed in Luxembourg

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

Contents

User guide 7
Mission statement 9
Foreword 11

1 2011 HIGHLIGHTS

1. 2011 HIGHLIGHTS 12

1.1. General overview of 2011 12
1.2. Results in 2011 16

2 SUPERVISION AND ENFORCEMENT

2. SUPERVISION AND ENFORCEMENT 18

2.1. Introduction 18
2.2. Data protection officers 18
2.3. Prior checks 19
2.3.1. Legal base 19
2.3.2. Procedure 20
2.3.3. Main issues in prior checks 22
2.3.4. Consultations on the need for prior checking 26
2.3.5. Notifications not subject to prior checking or withdrawn 26
2.3.6. Follow-up of prior checking opinions 27
2.3.7. Conclusions 27
2.4. Complaints 28
2.4.1. The EDPS mandate 28
2.4.2. Procedure for handling of complaints 28
2.4.3. Confidentiality guaranteed to the complainants 30
2.4.4. Complaints dealt with during 2011 31
2.5. Monitoring compliance 34
2.5.1. General monitoring and reporting: 2011 Survey 34
2.5.2. Targeted monitoring 34
2.5.3. Inspections 35
2.6. Consultations on administrative measures 37
2.6.1. Consultations Articles 28.1 and 46(d) 37
2.7. Data protection guidance 40
2.7.1. Thematic Guidelines 40
Guidelines on anti-harassment procedures 40
Guidelines on staff evaluation 41
Follow-up Report on Video-Surveillance Guidelines 41
2.7.2. Training 42

3 POLICY AND CONSULTATION

3. POLICY AND CONSULTATION 44

3.1. Introduction: overview of the year and main trends 44
3.2. Policy framework and priorities 45
3.2.1. Implementation of consultation policy 45
3.2.2. Results in 2011 46
3.3. Review of the EU Data Protection Framework 47
3.3.1. A comprehensive approach to personal data protection in the European Union 47
3.4. Area of Freedom, Security and Justice and international cooperation 48
3.4.1. Data Retention 48
3.4.2. Terrorist Finance Tracking System (TFTS) 49
3.4.3. European Passenger Name Records 49
3.4.4. Agreement between the EU and Australia on Passenger Name Records 50
3.4.5. Agreement between the EU and USA on Passenger Name Records 51
3.4.6. Anti-corruption package 51
3.4.7. Legislative proposals concerning certain restrictive measures 51
3.4.8. Migration 52
3.4.9. Victims of crime 52

3.5. Digital Agenda and technology **53**
3.5.1. Net neutrality 53
3.5.2. Technological project "Turbine" 53
3.6. Internal Market including financial data **54**
3.6.1. Internal Market Information System 54
3.6.2. Energy Market Integrity and Transparency 54
3.6.3. Interconnection of business registers 55
3.6.4. Credit agreements relating to residential property 55
3.6.5. Over-the-counter derivatives, central counterparties and trade repositories 56
3.6.6. Technical requirements for credit transfers and direct debits in Euros 56
3.6.7. Airport body scanners 57
3.7. Cross-border enforcement **57**
3.7.1. Intellectual Property Rights Enforcement Directive 57
3.7.2. Customs enforcement of intellectual property rights 58
3.7.3. Jurisdiction and the recognition and enforcement of judgments in civil and commercial matters 58
3.7.4. European Account Preservation Order 58
3.8. Public health and consumer affairs **59**
3.8.1. Consumer Protection Cooperation System 59
3.9. Other issues **59**
3.9.1. OLAF Reform Regulation 59
3.9.2. EU Financial Regulation 60
3.9.3. European statistics on safety from crime 60
3.9.4. Transport 60
3.9.5. Common Agricultural Policy after 2013 61
3.9.6. Fisheries policy control 62
3.10. Public access to documents containing personal data **63**
3.11. Court matters **63**
3.11.1. EDPS participation in court proceedings 63
3.11.2. Data protection case law 64
3.12. Future technological developments **64**
3.13. Priorities for 2012 **66**

4. COOPERATION 68

4.1. Article 29 Working Party **68**
4.2. Coordinated supervision of Eurodac **69**
4.2.1. Advance Deletion Report 70
4.2.2. New exercise in 2012: unreadable fingerprints 70
4.2.3. Coordinated security audit questionnaire 70
4.2.4. Visa Information System 70
4.3. Supervision of the Customs Information System (CIS) **71**
4.4. Police and judicial cooperation: cooperation with JSB/JSAs and WPPJ **71**
4.5. European Conference **72**
4.6. International Conference **73**

5. INFORMATION AND COMMUNICATION 74

5.1. Introduction **74**
5.2. Communication 'features' **74**
5.2.1. Key audiences and target groups 74
5.2.2. Language policy 74
5.3. Media relations **75**
5.3.1. Press releases 75
5.3.2. Press interviews 75
5.3.3. Press conference 76
5.3.4. Media enquiries 76
5.4. Requests for information and advice **77**
5.5. Study visits **78**
5.6. Online information tools **79**
5.6.1. Website 79
5.6.2. Newsletter 79

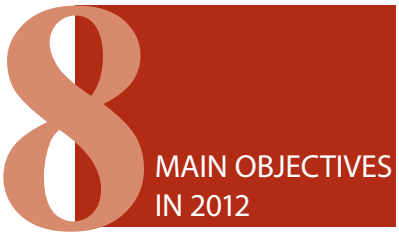
5.7. Publications **79**
5.7.1. Annual Report 79
5.7.2. Thematic publications 80
5.8. Awareness-raising events **80**
5.8.1. Data Protection Day 2011 80
5.8.2. EU Open Day 2011 81

6. ADMINISTRATION, BUDGET AND STAFF 82

6.1. Introduction **82**
6.2. Budget **82**
6.3. Human resources **83**
6.3.1. Recruitment 83
6.3.2. Traineeship programme 85
6.3.3. Programme for seconded national experts 85
6.3.4. Organisation chart 85
6.3.5. Working conditions 85
6.3.6. Training 85
6.3.7. Social activities 86
6.4. Control functions **86**
6.4.1. Internal control 86
6.4.2. Internal audit 87
6.4.3. External audit 87
6.4.4. Security 87
6.5. Infrastructure **87**
6.6. Administrative environment **88**
6.6.1. Administrative assistance and inter-institutional cooperation 88
6.6.2. Internal rules 89
6.6.3. Document management 89
6.6.4. Planning 89

7. EDPS DATA PROTECTION OFFICER 90

7.1. The DPO at the EDPS **90**
7.2. The Register of processing operations **90**
7.3. EDPS 2011 Survey **90**
7.4. Information and raising awareness **91**



8. MAIN OBJECTIVES IN 2012 92

8.1. Supervision and enforcement **92**
8.2. Policy and consultation **93**
8.3. Cooperation **93**
8.4. Other fields **94**

Annex A — Legal framework 95
Annex B — Extract from Regulation (EC) No 45/2001 97
Annex C — List of abbreviations 99
Annex D — List of Data Protection Officers 101
Annex E — List of prior check opinions 104
Annex F — List of opinions and formal comments on legislative proposals 109
Annex G — Speeches by the Supervisor and Assistant Supervisor in 2011 112
Annex H — Composition of EDPS Secretariat 115

USER GUIDE

Following this guide, there is a mission statement and foreword to the 2011 Annual Report by Peter Hustinx, European Data Protection Supervisor (EDPS), and Giovanni Buttarelli, Assistant Supervisor.

Chapter 1 — **2011 Highlights** presents the main features of the EDPS work in 2011 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 to 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 2011. It also includes thematic guidelines adopted by the EDPS in anti-harassment procedures and staff evaluation, as well as the follow-up report on video-surveillance.

Chapter 3 — **Consultation** deals with developments in the EDPS 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 discusses the involvement of the EDPS in cases before the Court of Justice. 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 work done 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 — **Communication** presents the EDPS information and communication activities and achievements, including external communication with the media, awareness-raising events, public information and online information tools.

Chapter 6 — **Administration, budget and staff** details the key areas within the EDPS organisation including budget issues, human resource matters and administrative agreements.

Chapter 7 — **EDPS Data Protection Officer (DPO).** Drawing on the DPO action plan and the implementing rules adopted, this chapter highlights the progress made on the Register of notifications, on compliance with the *Spring exercise* and on the need for information and raising awareness.

Chapter 8 - **Main objectives in 2012** provides a brief look ahead and the main priorities for 2012.

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 is also available, providing an overview of key developments in EDPS activities over 2011.

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.

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).

MISSION STATEMENT

The mission of the European Data Protection Supervisor (EDPS) is to ensure that the fundamental rights and freedoms of individuals — in particular their privacy — are respected when the EU institutions and bodies process personal data.

The EDPS is responsible for:

- monitoring and ensuring that the provisions of Regulation (EC) No 45/2001 [1], as well as other EU acts on the protection of fundamental rights and freedoms, are complied with when EU institutions and bodies process personal data (supervision);
- advising EU institutions and bodies on all matters relating to the processing of personal data; this includes consultation on proposals for legislation and monitoring new developments that have an impact on the protection of personal data (consultation);
- cooperating with national supervisory authorities and supervisory bodies in the former 'third pillar' of the EU with a view to improving consistency in the protection of personal data (cooperation).

In light of this, the EDPS also aims to work strategically to:

- promote a 'data protection culture' within EU institutions and bodies, thereby contributing to improve good governance;
- integrate respect for data protection principles in EU legislation and policies, whenever relevant;
- improve the quality of EU policies, whenever effective data protection is a basic condition for their success.

[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 of the European Parliament and of the Council and Article 16 of the Treaty on the Functioning of the European Union, which has replaced Article 286 of the EC Treaty.

This report covers 2011 as the seventh full year of activity of the EDPS as an independent supervisory authority, tasked with ensuring 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. It also covers the third year of our common mandate as members of this authority.

In the course of 2011, we 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 are making good progress in complying with the Data Protection Regulation, while others should increase their efforts.

In the consultation of new legislative measures, we issued a record number of opinions on a range of subjects. The most prominent is the Review of the EU legal framework for data protection, which remains high on our agenda. However, the implementation of the Stockholm programme in the area of freedom, security and justice and the Digital Agenda, as the cornerstone for the Europe 2020 strategy, also had an impact on data protection. This can be said as well of issues in the internal market, public health and consumer affairs, and enforcement in a cross border context.

At the same time, we increased cooperation with other supervisory authorities and further improved the efficiency and effectiveness of our organisation.

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. The level of quality is outstanding and our staff contributes greatly to our effectiveness.

Peter Hustinx
European Data Protection Supervisor

Giovanni Buttarelli
Assistant Supervisor

1 2011 HIGHLIGHTS

1.1. General overview of 2011

The main activities of the EDPS in 2011 have been based on the same overall strategy as in past years, though they have continued to grow both in scale and scope. The capacity of the EDPS to act both effectively and efficiently has also been improved.

The legal framework([2]) within which the EDPS acts provides for a number of tasks and powers which allow for a distinction between three main roles. These roles continue to serve as strategic platforms for the activities of the EDPS and are reflected in the mission statement:

- **a supervisory role** to monitor and ensure that EU institutions and bodies([3]) comply with existing legal safeguards whenever they process personal data;
- **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 data;
- **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 data.

These roles will be detailed further in Chapters 2, 3 and 4 of this annual report, in which the main activities of the EDPS and the progress achieved in 2011 are presented. Some key elements are summarised in this section.

The importance of information and communication concerning these activities justifies a separate emphasis on communication and this is covered in Chapter 5. All these activities rely on effective management of financial, human and other resources, as outlined in Chapter 6.

Supervision and enforcement

Supervisory tasks range from advising and supporting data protection officers through prior checking of risky data processing operations, to conducting inquiries, including on-the-spot inspections and handling complaints. Further advice to the EU administration can also take the form of consultations on administrative measures or the publication of thematic guidelines.

All EU institutions and bodies must have at least one **data protection officer** (DPO). In 2011, the number of DPOs totalled 54. Regular interaction with them and their network is an important condition for effective supervision. The EDPS has worked closely with the 'DPO quartet' composed of four DPOs (Council, European Parliament, European

([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

Commission and the European Food Safety Agency) who coordinate the DPO network. The DPO network meetings, which the EDPS attends, are an opportunity to give updates on EDPS work, give an overview of developments in EU data protection and to discuss issues of common interest.

Prior checking of risky processing operations continued to be an important aspect of supervision. In 2011, the EDPS received 164 notifications for prior checking and adopted 71 prior check opinions on standard administrative procedures, such as staff evaluation, administrative inquiries, disciplinary procedures and anti-harassment procedures, but also on core business activities such as the Consumer Protection System, the Quality Management System and ex-post quality checks at OHIM and the Electronic Exchange of Social Security system at the European Commission. These opinions are published on the EDPS website and their implementation is followed up systematically.

In 2011, the number of **complaints** received by the EDPS increased to 107; 26 of these were found to be admissible. Many inadmissible complaints involved issues at national level for which the EDPS is not competent. In the 15 cases resolved during 2011, the EDPS found that either there was no breach of data protection rules or that the necessary measures to comply were undertaken by the controller. Conversely in two cases, non-compliance with data protection rules was found to have occurred and recommendations were made to the controller.

The **implementation of the Regulation** by institutions and bodies is also monitored systematically by regular stock taking of performance indicators, involving all EU institutions and bodies. The EDPS launched his third stock taking exercise, monitoring compliance with data protection rules (2011 Survey) leading to a report highlighting the progress made by institutions and bodies in implementing the Regulation and also underlining shortcomings. In addition to this general exercise, targeted monitoring exercises were carried out in cases where, as a result of supervision activities, the EDPS had cause to be concerned about the level of compliance in specific institutions or bodies. These took the form of correspondence with the institution or body or a one day visit notably to the European Railway Agency, the Community Plant Variety Office, the European Foundation for the Improvement of Living and Working Conditions and the European Global Navigation Satellite Systems Agency.

The EDPS also carried out an on-the-spot inspection at the CEDEFOP, OLAF and the ECB to verify compliance on specific issues.

Further work was also done in response to **consultations on administrative measures** by EU institutions and bodies in relation to the processing of personal data. A variety of issues were raised, including publication of employees' pictures on the Intranet, controllership when CCTV is operated on the premises of another institution and the processing of employees' e-mails.

The EDPS also adopted **guidelines** on anti-harassment procedures and staff evaluation and followed up on the progress made by institutions and bodies following the Video-Surveillance Guidelines.

Consultation

2011 was a busy year for consultation, leading to a record number of 24 opinions, 12 formal comments and 41 informal comments. The EDPS continued to implement a proactive approach to consultation, based on a regularly updated inventory of legislative proposals to be submitted for consultation as well as availability for informal comments in the preparatory phases of legislative proposals. Taking advantage of this availability for informal comments, in 2011 the Commission services almost doubled the number of informal consultations compared to 2010.

The Commission's work on a modernised legal framework for data protection in Europe merits special mention. The legislative review process has been closely followed by the EDPS, who provided input at different levels, including an opinion on the Commission Communication laying down a comprehensive approach to data protection in Europe in January and informal comments on the draft legislative proposals in December.

There appears to be a general diversification in the fields touching on data protection issues: besides traditional priorities such as the Area of Freedom, Security and Justice (AFSJ) and international data transfers, new areas are emerging, as may be seen in the large number of opinions adopted relating to the internal market. The following highlights include a selection of the opinions adopted in the respective fields.

In the **AFSJ**, the EDPS issued several highly critical opinions on issues such as the evaluation report

on the data retention directive 2006/24/EC and the proposal for European Passenger Name Records processing. Passenger name records were also the subject of two opinions dealing with the agreements for the transfer of such data to Australia and the USA respectively. The EDPS also commented on the Commission communication on a Terrorist Finance Tracking System (TFTS), questioning its necessity.

Regarding **Information Technology and the Digital Agenda**, the EDPS published an innovative opinion on net neutrality highlighting the impact of some monitoring practices by internet service providers. He also issued his first ever opinion on an EU-funded research project which dealt with privacy-preserving ways of implementing biometrics.

In the area of the **internal market**, the EDPS issued, among others, an opinion on the Internal Market Information System (IMI), urging that new functionalities to be added in the future be clarified. Other notable opinions were issued on Energy market integrity and transparency as well as over-the-counter derivatives, central counterparties and trade repositories. In these cases, the proposals intended to grant far-reaching investigation powers that were not clearly circumscribed to regulatory authorities and so the EDPS called for greater clarity.

Several opinions were issued on **enforcement in a cross-boder context.** The EDPS provided, for instance, guidance on the proposals for the intellectual property rights enforcement directive, calling for the establishment of a clear retention period as well as for clarifying the legal basis of an associated database. Regarding the proposal for the European account preservation order, he emphasised the need to limit the personal data processed to the minimum necessary.

In **public health and consumer affairs**, the EDPS issued an opinion on the Consumer Protection Cooperation System (CPCS), urging the legislator to reconsider the retention periods and to explore ways of ensuring privacy by design.

The EDPS also intervened in other areas, such as the OLAF reform regulation, the EU financial regulation and the use of digital tachographs for professional drivers.

Court cases

In 2011, the EDPS intervened in five cases before the General Court and the Civil Service Tribunal.

One of the cases dealt with an allegedly illegal transfer of medical data between the medical services of the Parliament and the Commission. The Civil Service Tribunal - taking this initiative for the first time - invited the EDPS to intervene. In its judgment, the Tribunal followed the EDPS reasoning and awarded financial compensation to the applicant.

Three other cases dealt with access to documents of EU institutions and can be seen as follow-up to the *Bavarian Lager* ruling. In all three, the EDPS argued in favour of greater transparency. This reasoning was followed by the Court in one case; in another case, it upheld the Parliament decision not to grant access; the third case is, at the time of writing, pending.

In addition, the EDPS intervened in an infringement proceeding against Austria on the independence of DPAs. In his intervention, he argued that the organisation structure of the office of the Austrian DPA as provided for in national law, does not live up to the standard of independence required by Directive 95/46/EC. At the time of writing, this case too is pending.

Cooperation

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

The EDPS and the Article 29 Working Party have worked well together on a range of subjects, especially in the context of the subgroups on key provisions and borders, travel and law-enforcement (BTLE). In the former, the EDPS was the *rapporteur* for the opinion on the notion of 'consent'.

In addition to the Article 29 Working Party, the EDPS continued his close cooperation with the authorities established to exercise **joint supervision on EU large-scale IT systems**.

An important element of these cooperative activities is **Eurodac**. The Eurodac Supervision Coordination Group – composed of national data protection authorities and the EDPS – met in Brussels in June and October 2011. The Group completed a coordinated inspection on the issue of advance deletion, further elaborated a joint framework for the planned full security audit and scheduled another coordinated inspection, the results of which will be reported in 2012. In addition, the group informally discussed the issue of coordinated supervision of the Visa Information System (VIS), which went live in October 2011.

A similar arrangement governs the supervision of the **Customs Information System** (CIS), in the context of which the EDPS convened two meetings of the CIS Supervision Coordination Group in 2011. The meetings gathered the representatives of national data protection authorities, as well as representatives of the Customs Joint Supervisory Authority and Data Protection Secretariat. In the meeting in June, the Group adopted an action plan outlining its planned activities for 2011 and 2012, while in the December meeting, it agreed on its first two coordinated inspections. The results of these inspections will be delivered during the course of 2012.

Cooperation in **international fora** continued to attract attention, especially the European and International Conferences of Data Protection and Privacy Commissioners. In 2011, the European Conference was held in Brussels, hosted by the Article 29 Working Party and the EDPS. In Mexico City, privacy and data protection commissioners from around the world adopted a declaration calling for efficient cooperation in a world of 'big data'.

Some EDPS key figures in 2011

➔ 71 prior-check opinions adopted, 6 non prior check opinions

➔ 107 complaints received, 26 admissible. Main types of violations alleged: violation of confidentiality of data, excessive collection of data or illegal use of data by the controller

➔ 34 consultations on administrative measures. Advice was given on a wide range of legal aspects related to the processing of personal data conducted by the EU institutions and bodies

➔ 4 on-the-spot inspections carried out

➔ 2 guidelines published on anti-harassment procedures and evaluation of staff

➔ 24 legislative opinions issued on, among others, initiatives relating to the Area of Freedom, Security and Justice, technological developments, international cooperation, data transfers, or internal market.

➔ 12 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.

➔ 41 sets of informal comments

➔ 14 new colleagues recruited

1.2. Results in 2011

The following main objectives were set out in 2010. Most of these objectives have been fully or partially realised in 2011. In some cases, work will continue in 2012.

- **Raising awareness**

The EDPS invested time and resources in awareness raising exercises for EU institutions and bodies and DPOs. This took the form of thematic guidance notably in the areas of anti-harassment procedures, staff evaluation and workshops on data protection for DPOs or controllers.

- **Role of prior checking**

In 2011, the EDPS received 164 notifications for prior checking, the second highest number ever. This increase was due mainly to the launching of visits to agencies, on the spot inspections and the issuance of thematic guidance. The notifications received from newly created agencies also contributed to this increase. The EDPS continued to place strong emphasis on the implementation of recommendations made in prior check opinions.

- **Monitoring and reporting exercises**

The EDPS launched his third stock taking exercise, monitoring the compliance of data protection rules (2011 Survey). In addition to this general exercise, targeted monitoring exercises were carried out in cases where, as a result of supervision activities, the EDPS had cause for concern about the level of compliance in specific institutions or bodies. Some of these were correspondence based, whilst others took the form of a one day visit to the body concerned, with the aim of addressing compliance failings.

- **Inspections**

Inspections are a crucial tool, enabling the EDPS to monitor and ensure the application of the Regulation. In 2011, the EDPS launched four inspections and continued the follow up of recommendations made in previous inspections. A security audit of the Visa Information System (VIS) was also carried out.

- **Scope of consultation**

The EDPS again increased his output, issuing a record number of 24 opinions and 12 sets of formal comments. In many cases, the Commission had already consulted the EDPS before the adoption of its proposals, leading to 41 sets of informal comments being issued. Many of the opinions were followed up by presentations in the LIBE Committee of the European Parliament or the relevant Council Working Parties. The proposals for which opinions were published were selected from a systematic inventory of relevant subjects and priorities for the EDPS. The opinions, formal comments and the inventory are published on the EDPS website.

- **Review of the data protection legal framework**

The EDPS issued an opinion on the Commission Communication on a comprehensive approach on personal data protection, as well as informal comments on the legislative proposals. He closely followed the process and gave input where necessary and appropriate.

- **Implementation of the Stockholm Programme**

The EDPS closely followed policy developments related to the Stockholm Programme, issuing an opinion on the proposal for a directive on the use of PNR for law enforcement purposes, as well as formal comments on the introduction of a European Terrorist Financing Tracking Programme (TFTS). While no legislative proposals were issued on the topic of smart borders, the EDPS addressed the issue in his opinion on the Commission communication on migration.

- **Initiatives in the area of technology**

The EDPS issued his first opinion on an EU-funded research project; the project dealt with the privacy preserving implementation of biometrics. In the context of the Digital Agenda, he published an opinion on net neutrality.

- **Other initiatives**

The EDPS issued a variety of opinions and comments on other initiatives that had an impact on the protection of personal data, such as the Internal Market Information System and the use of security scanners at airports.

- **Cooperation with data protection authorities**

The EDPS actively took part in the work of the Article 29 Data Protection Working Party, especially in the subgroups on key provisions and on borders, travel and law enforcement.

- **Coordinated supervision**

The EDPS provided the data protection authorities involved in the coordinated supervision of Eurodac and the Customs Information System with an efficient secretariat. For the Visa Information System, the data protection authorities represented in the supervision coordination group had a first exchange of views as part of one of the Eurodac coordinated supervision meetings, addressing implications of the system and the approach to supervision.

- **Internal organisation**

Following the reorganisation of the Secretariat in 2010, the institution decided to launch a strategic review of all its activities in 2011, steered by a "Strategic Review" Task Force made up of the Director and representatives from all teams and disciplines. The first phase of the review culminated in an internal meeting of the institution in October 2011, which allowed the members and staff to reflect on their tasks, values and objectives.

- **Resource management**

The EDPS, in cooperation with the Parliament, carried out an exhaustive examination of the market for providers of a Case Management System and chose the contractor with the most appropriate product. At the end of 2011, the contract was signed and the work of developing a customised system began.

During 2011, work continued on the integration of the EDPS into IT applications in the field of human resources on the basis of Service Level Agreements: Syslog Formation was successfully introduced, work began on SysperII and an agreement was found on the introduction of MIPS in 2012.

2 SUPERVISION AND ENFORCEMENT

2.1. Introduction

The task of the EDPS in his independent supervisory capacity is to monitor the processing of personal data 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.

The EDPS continued to perform his main operational activities notably in the field of prior checks, complaints and consultations on administrative measures through 2011. The prior checking of processing operations which exhibit specific risks continued to represent an important aspect of supervision work at the EDPS in 2011, notably due to an increase in the number of notifications received. The number and complexity of complaints received also increased and led to a resolution of 15 cases in 2011. Within the framework of consultations on administrative measures, the EDPS examined a variety of issues.

Aside from his regular supervision activities, the EDPS also developed other forms of monitoring compliance with the Regulation, in line with the Compliance and Enforcement Policy adopted in December 2010. In addition to his general stock taking exercise, targeted monitoring exercises were carried out in cases where, as a result of supervision activities, the EDPS 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.

The EDPS also continued his awareness raising activities, notably by organising specific training for DPOs either in the form of a workshop or a teleconference and by producing thematic guidance for institutions and bodies in the field of anti-harassment procedures and staff evaluation.

2.2. Data protection officers

European Union institutions and bodies have an obligation to appoint a data protection officer (DPO) (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). A number of institutions have appointed data protection coordinators in order to coordinate all aspects of data protection within a particular directorate or unit.

In 2011, six new DPOs were appointed within new agencies or joint undertakings, bringing the total number of DPOs to 54. There was also a high turnover in institutions and established agencies, as many mandates expired this year.

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 2011.

A 'DPO quartet' composed of four DPOs (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 April 2011 at the Fundamental Rights Agency in Vienna and at the European Ombudsman in Strasbourg in October 2011. The EDPS took the opportunity to update the DPOs on his work, give an overview of recent developments in EU data protection and discuss issues of common interest.

More specifically, the EDPS used this forum to discuss the procedures and tools for prior checks; present recent developments in data protection; update the DPOs on the review of the legal framework; present thematic guidelines and the 2011 Survey; provide information on training initiatives and share progress on the video-surveillance guidance report. The forum is also used to share initiatives for European Data Protection Day (on 28 January).

On 8 June 2011, the EDPS organised a workshop for DPOs as part of his guidance programme (see also Section 2.7.2). The aim was to provide basic training for DPOs, in particular those recently-appointed. The programme included an introduction to the basic principles and definitions of the Regulation and presentations on specific subjects such as the legal basis of data processing, rights of the data subject, transfer of data and processing on behalf of the controller. These presentations were supported by concrete examples taken from the EDPS' supervision activities. The afternoon session was dedicated to cooperation between DPOs and the EDPS, focusing on the practical aspects of complaint handling, prior checking procedures and security of processing operations. The workshop was well-attended and active participation of the DPOs led to a productive exchange of experiences and concerns.

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. During the reporting period, the EDPS continued to apply the criteria developed in previous years([4]) when interpreting this provision, both when deciding that a notification

([4]) See Annual Report 2005, section 2.3.1.

30th DPO Meeting in Strasbourg in October 2011.

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

Notification

Prior checks must be carried out by the EDPS following receipt of a notification from the DPO. Should the DPO be in 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.

Period, suspension and extension

The EDPS must deliver his opinion within two months of receiving the notification([5]). Should the EDPS make a request for further information, the period of two months is usually suspended until the EDPS has obtained this information. This period of suspension includes the time given to the DPO for comments and if needed, further information on the final draft. In complex cases, the EDPS may also extend the initial period by a further two months. If no decision has been delivered at the end of the two-month period or extension thereof, the opinion of the EDPS is deemed to be favourable. To date, no such tacit opinion has ever arisen.

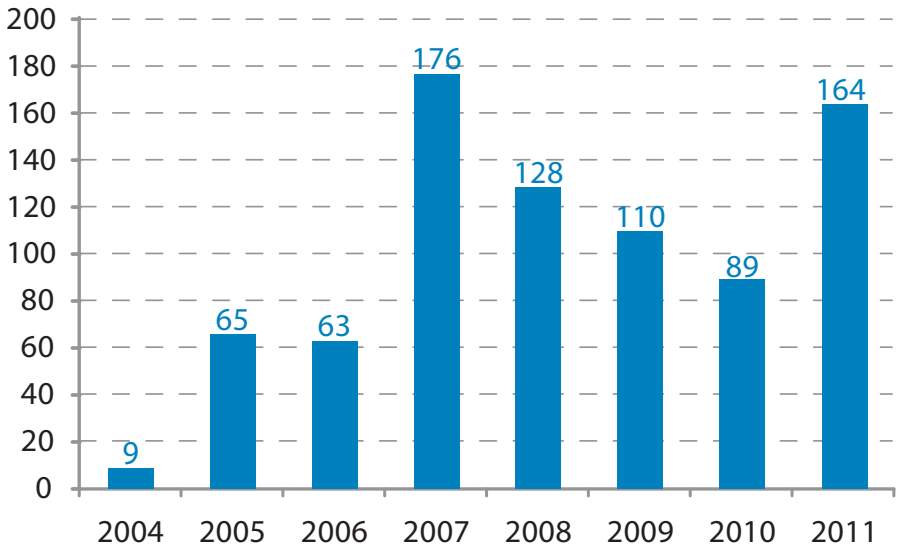
([5]) For ex-post cases received before 1 September 2011, the month of August was not included in the calculation of deadlines for institutions and bodies, nor for the EDPS.

Register

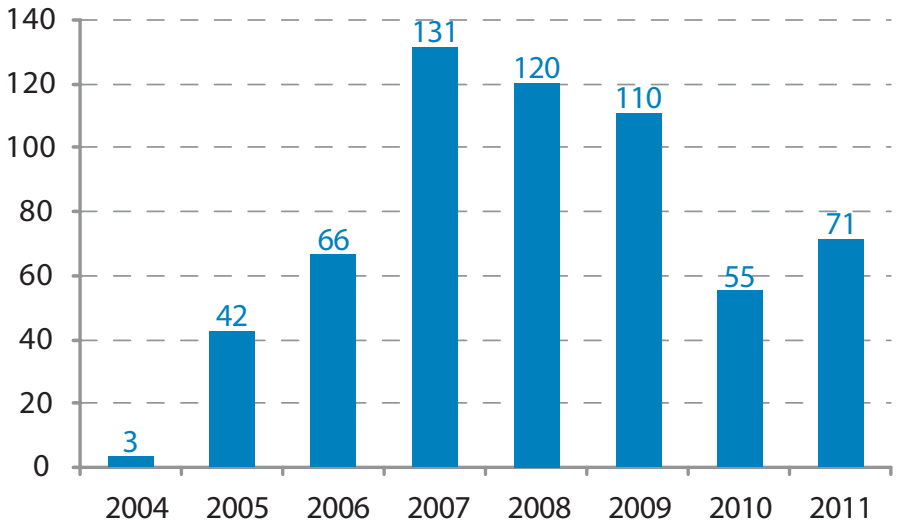
In 2011, the EDPS received 164 notifications for prior checking - the second highest number ever. This represents a dramatic increase with almost twice as many notifications received in 2011 compared to 2010. Whilst the EDPS has cleared the backlog of *ex-post* prior checks for most EU institutions, 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 2011 have generated an increase in the number of notifications.

Under the Regulation, the EDPS must keep a register of all processing operations of which he has been notified for prior checking (Article 27(5)). This register contains the information referred to in Article 25 and is available to the public, in the interests of transparency, on the EDPS website (except for security measures, which are not mentioned in the public register).

Notifications to the EDPS



EDPS prior-check opinions per year



Opinions

The final position of the EDPS takes the form of an opinion, which is notified to the controller of the processing operation and the DPO of the institution or body (Article 27(4)). In 2011, the EDPS issued **71 prior checking opinions** and **6 on 'non-prior checks'** (see Section 2.3.5). This represents a significant increase compared to the previous year and also takes into account that the EDPS dealt with a significant number of cases with joint opinions: in 2011, there were 10 joint opinions dealing with a total of 52 notifications (e.g. one joint opinion on health data dealing with a total of 18 notifications). In issuing these joint opinions following the publication of guidelines, for example on health data and anti-harassment, the EDPS thus increased efficiency at the cost of statistical visibility.

As was the case in 2010, a **significant number of these opinions** were addressed to the **European Commission**, with 16 prior checking opinions (and three non-prior checks). Unlike in previous years where the other large EU institutions (European Parliament and Council) had been frequent addressees in 2011, the runners-up were EU agencies and bodies, to which the EDPS addressed an unprecedented number of opinions (partially in the form of joint opinions), e.g. six relating to processing operations at the Community Plant Variety Office, five to the European Foundation for the Improvement of Living and Working Conditions and three or four to several other EU agencies. EU agencies have thus further continued to notify their core business activities and standard administrative procedures according to the relevant procedures drawn up by the EDPS (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 the EDPS may of course also exercise other powers granted to him under Article 47 of the Regulation. For example, the EDPS introduced a temporary ban on a processing operation which was found to be in breach of the data protection principles (see Section 2.3.3.10).

Once the EDPS has delivered his opinion, it is made public. All published opinions are available on the website of the EDPS in three language versions (as these become available) together, in most cases, with a summary of the case.

A case manual ensures that the entire team works on the same basis and that the opinions of the EDPS are adopted after a complete analysis of all significant information. It provides a template for opinions, based on accumulated practical experience and is continuously updated. A workflow system is used to make sure that all recommendations in a particular case are followed up and, where applicable, all enforcement decisions are complied with (see Section 2.3.6).

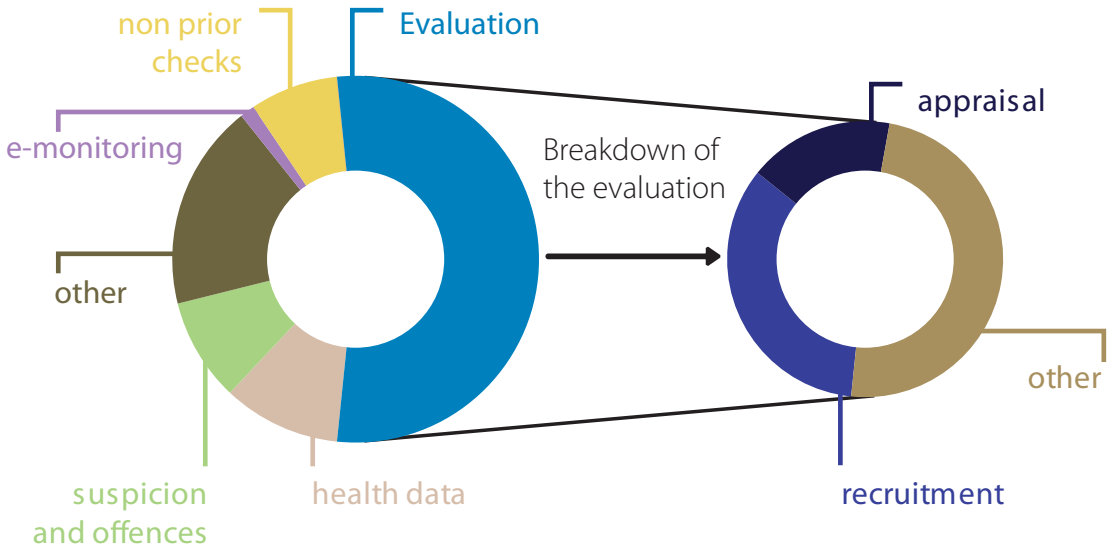
Procedure for *ex-post* prior checks in EU agencies

In October 2008, the EDPS launched a new procedure for *ex-post* prior checks in EU agencies. Since standard procedures are the same in most EU agencies and are based on Commission decisions, notifications on a similar theme are gathered and either a collective opinion (for various agencies) or a 'mini prior check' addressing only the specific needs of each individual agency is adopted. To help the agencies complete their notifications, the EDPS summarises 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 first theme was **recruitment** and led to a horizontal opinion of the EDPS 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, the EDPS 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 (on thematic guidance, see Section 2.7).

2.3.3. Main issues in prior checks

Opinions 2011 per main category



2.3.3.1. Processing of health data in the workplace

Following the publication of **EDPS Guidelines** on the processing of health data in the workplace, the EDPS carried out a particularly challenging exercise in examining 18 notifications for prior checking regarding the processing operations in 18 agencies on pre-recruitment examinations, annual check-ups and sick leave absences. In view of the similarities in procedures and data protection practices, the EDPS decided to issue one joint opinion on 11 February 2011 (Case 2010-0071).

The joint opinion on the processing of health data at the workplace highlighted three crucial issues:

- firstly, the **broad concept of "health data"** and the impact of data protection principles on processing operations related to pre-recruitment examinations, annual check-ups and sick leave absences;
- secondly, the absence of important elements in the contracts of several agencies with external medical providers, notably of security measures and data protection clauses in the light of Article 23 of the Regulation;
- thirdly, the incomplete scope of privacy statements used: for the processing to be lawful under Articles 11 and 12 of the Regulation, the controller shall inform the data subject about *all* elements related to the processing operations, in particular where the processing is based on the consent of the data subject.

EU institutions, agencies and bodies process health-related data.

2.3.3.2. Consumer Protection Co-operation System (CPCS)

The Consumer Protection Co-operation System (CPCS) is an information technology system designed and operated by the Commission, which facilitates co-operation among Member State authorities and the European Commission in the area of consumer protection pursuant to Regulation (EC) No 2006/2004 on consumer protection cooperation. On 4 May 2011, the EDPS issued a prior checking opinion concerning the exchange of information including personal data by competent authorities in the framework of this co-operation (Case 2009-0019).

Modern information technologies support consumer protection.

The European Commission has a central role in configuring the CPCS system architecture and operating the system and is subject to the supervision of the EDPS. In his opinion, the EDPS recommended technical and organisational measures to be taken by the European Commission. Many of the recommendations provided in the opinion - including those on training, the establishment of data protection guidelines, information to data subjects and **"privacy by design" solutions built into the system architecture** - should also facilitate compliance with data protection rules by other users of the system, such as competent authorities in Member States.

2.3.3.3. Quality Management System and ex-post quality checks at OHIM

Since 2007, the Office of Harmonization for the Internal Market (OHIM) has been conducting ex-ante and ex-post quality checks of trademark decisions produced by OHIM's trademark examiners for quality control purposes. The results of these checks show the types of mistakes made by examiners. In September 2009, OHIM informed examiners that the results of ex-post quality checks (EPQC) would also be used for the purpose of their annual performance appraisal. As a result, the EPQC system was submitted for prior checking to the EDPS, who issued his opinion on 9 June 2011 (Case 2010-0869).

Given the **change of purpose** of the processing from general quality control to individual performance appraisal, in his opinion the EDPS recommended that OHIM adopts an internal decision setting forth appropriate **data protection guarantees** and ensures that EPQC data are not the sole basis for the annual performance appraisals of examiners. The EDPS furthermore recommended measures to ensure the accuracy of the data, to inform the examiners about the processing and to ensure that they are granted all their rights as data subjects.

2.3.3.4. Access Control System – Joint Research Centre (JRC) - Ispra site

The purpose of the Access Control System at the Ispra site of the Joint Research Centre (JRC) is to protect the premises against unauthorised access and external and internal threats. The trigger for the prior checking procedure was that biometric readers covered access to some protected areas, although these were not used by many staff members. The EDPS issued an opinion on 15 July 2011 (Case 2010-0902).

The EDPS concluded that the European Commission was in **breach of the Regulation** since it had installed and operated a biometric access control system without notifying this processing operation to the EDPS ex-ante. Moreover, the EDPS recommended that the JRC should, among other things:

- enact a legal basis for the processing operations by the access control system using biometrics;

- comply with the CCTV Guidelines and report to the EDPS on the measures it has implemented in that respect;

- reconsider the technological choices made by means of an **impact assessment**, including a timetable to implement changes in technology.

2.3.3.5. Fingerprint recognition study by JRC of children below the age of 12 years

The Joint Research Centre (JRC) conducted a study entitled "Fingerprint recognition study of children below the age of 12 years" within the scope of the European Visa Information System (VIS). The study examined the physiological development of the fingertip ridge structure of children (ridge distance, position of minutiae) and the resulting recognition rate of fingerprint matching algorithms adapted to children. As this processing is related to biometric data, prior checking was required to allow the EDPS to verify that stringent safeguards had been implemented; he published his opinion on 25 July 2011 (Case 2011-0209).

Fingerprint recognition is one of the most well-known biometrics and refers to an automated method of verifying a match between two human fingerprints.

The EDPS recognised the importance of the biometric study, but highlighted the need for the data controller to perform a **risk assessment** and establish an **access policy** relating to the processing operation at stake.

2.3.3.6. Electronic Exchange of Social Security Information - European Commission

The EDPS prior checked an IT system for the cross-border exchange of social security information developed by the European Commission. The system, which is expected to be operational as of 2012, aims to facilitate the calculation and payment of social security benefits for persons who have worked in more than one Member State and allows for a more efficient verification of data.

In his opinion of 28 July 2011 (Case 2011-0016), the EDPS welcomed the proposal to create a 'one stop point' for individuals wanting to exercise their rights. The EDPS nevertheless invited the European Commission to ensure that data subjects can fully enforce their rights at the relevant contact point in the Member State. To ensure the security of the data, the EDPS also recommended a number of technical measures, which include the recommendation that only encrypted data should be transmitted to prevent the European Commission from having access to the content of the sensitive data transiting through the system. Since the system is still in its production phase, the EDPS emphasised that he should be notified of any substantial change to the design of the system which could impact the level of data protection.

2.3.3.7. Physical Access Control System - European Commission

The European Commission's physical access control system (PACS) performs all physical security functions and is based on the use of **biometric data**. The use of such data presents specific risks to the rights and freedoms of data subjects, due to some **inherent characteristics of this type of data**. For example, biometric data irrevocably changes the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use. These risks justify the need for such data processing to be prior checked by the EDPS in order to verify that stringent safeguards have been implemented. The EDPS issued his opinion on 8 September 2011 (Case 2010-0427).

The EDPS welcomed the European Commission's involvement of the EDPS at a very early stage, thus facilitating the development of a privacy-friendly approach in implementing the processing operations at stake. Among other aspects of the PACS, the EDPS focused his analysis on the categories of data subjects concerned, the existence of fallback procedures for individuals who are not eligible, even temporarily, for enrolment (e.g. because of damaged fingerprints), retention periods and the security measures implemented.

2.3.3.8. "IDEAS-Exclusion of Experts by Applicants" project - ERCEA

Project proposals submitted to the European Research Council Executive Agency (ERCEA) are subject to peer evaluation i.e. a review by panels composed of independent scientists and scholars. The EDPS opinion of 21 September 2011 (Case 2010-0661), regards a procedure notified by the ERCEA under which applicants submitting a project proposal can request that up to three specific persons would *not* act as peer reviewer in the evaluation of the proposal. The purpose of the processing is to guarantee a fair, equal and objective assessment of project proposals and neutralise any concerns on the correctness of the evaluation outcome and the objectivity of experts.

In light of **principle of data quality**, the EDPS invited ERCEA to consider defining pre-fixed categories rather than using a "free text" field for submitting specific reasons to exclude certain peers from becoming panel members. The EDPS further recommended that ERCEA procedurally ensures that the rights of access and rectification of experts concerned are limited only to cases where this is necessary. Subject to the restrictions of Article 20 of the Regulation, each expert should, for example, be able to verify whether he/she wants to add his/her own statement "neutralising" or "balancing" the subjective appreciation by the applicant.

2.3.3.9. Systems enhancing cooperation between customs authorities - OLAF

Using the same platform, three systems (the Virtual Operational Cooperation Unit, the Mutual Assistance Broker and the Customs Information System) aim to enhance cooperation between customs authorities in the Member States, the European Commission and in some cases third countries and international organisations. To this end, they allow the exchange of information on persons, companies and goods under suspicion of infringing customs and agricultural legislation, in order to request connected authorities to take certain actions (e.g. specific checks, discreet surveillance). The systems involve the processing of sensitive data (suspicion of criminal behaviour, health data).

In his joint opinion of 17 October 2011 on the three systems (joint cases 2010-0797, 2010-0798, 2010-0799), the EDPS asked OLAF to provide better information to data subjects and recommended an evaluation of the need to process certain data categories as well as the retention periods applicable.

2.3.3.10. "Return to Work" policy - EU-OSHA

To facilitate the return to work of sick staff members, under the "Return to Work" policy of the European Agency for Safety and Health at Work (EU-OSHA), the staff member's Head of Unit or the Human Resources Section (HR) is responsible for coordinating actions between the staff member, his/her general practitioner, occupational health, HR and any other stakeholders (e.g. union and staff representatives). This involves regular contacts with the sick staff member, referrals for medical assessment and individual-level therapies (e.g. psychotherapy) and the examination of the staff member's job and medical assessments, which may result in redeployment or an adjustment of the staff member's working time, responsibilities and tasks.

In his opinion of 24 October 2011 (Case 2011-0752), the EDPS concluded that some elements of the processing operation breached the principle of necessity and proportionality and violated the data quality principles of adequacy, relevance, proportionality and accuracy and therefore imposed a **temporary ban on the processing**. The EDPS noted that, whilst the stated purpose of the processing referred to fitness to work from an occupational and preventive medicine perspective, only medical specialists - not the Head of Unit or HR- are able to certify these aspects. Further concerns regarded how the EU-OSHA could ensure that any consent from the data subjects was informed and freely given under the circumstances and that only adequate, relevant and not excessive data should be collected, processed and transferred.

2.3.4. Consultations on the need for prior checking

The mere possibility of the presence of **sensitive data** in a case does not automatically subject it to prior checking. Nevertheless, the processing of sensitive data relating to, for example, health or criminal/civil offences does mean that particular attention should be given to the adoption of appropriate security measures, in accordance with Article 22 of the Regulation.

When in doubt, EU institutions and bodies can consult the EDPS on the need for prior checking under Article 27(3) of the Regulation. During 2011, the EDPS received 13 such consultations from DPOs. Among the issues considered by the EDPS were processing activities regarding mobility in the context of restructuring and the use of electronic communication (mobile telephony, email and internet).

2.3.5. Notifications not subject to prior checking or withdrawn

Following careful analysis, six cases were found not to be subject to prior checking in 2011. In these situations (also referred to as 'non-prior checks'), the EDPS may still make recommendations. Furthermore, one notification was withdrawn and one was replaced.

In his opinion of 12 November 2009 (Case 2009-0477), regarding the planned verification of flexitime clocking operations through data on physical access collected by the European Council, the EDPS confirmed his doubts regarding the proportionality of the planned processing operation. He advised that the operation would violate the Regulation at various levels (lawfulness of the processing operation, necessity and proportionality, change in purpose, data quality) if the verification of flexitime clocking operations with respect to data on physical access checks, as described in the notification, were to be executed outside the framework of an administrative investigation. On 6 July 2011, the EDPS received a letter from the Data Protection Officer of the European Council informing him that, following the above EDPS prior check opinion, the data controller had ***withdrawn the notification*** *and the planned system had not been implemented.*

2.3.6. Follow-up of prior checking opinions

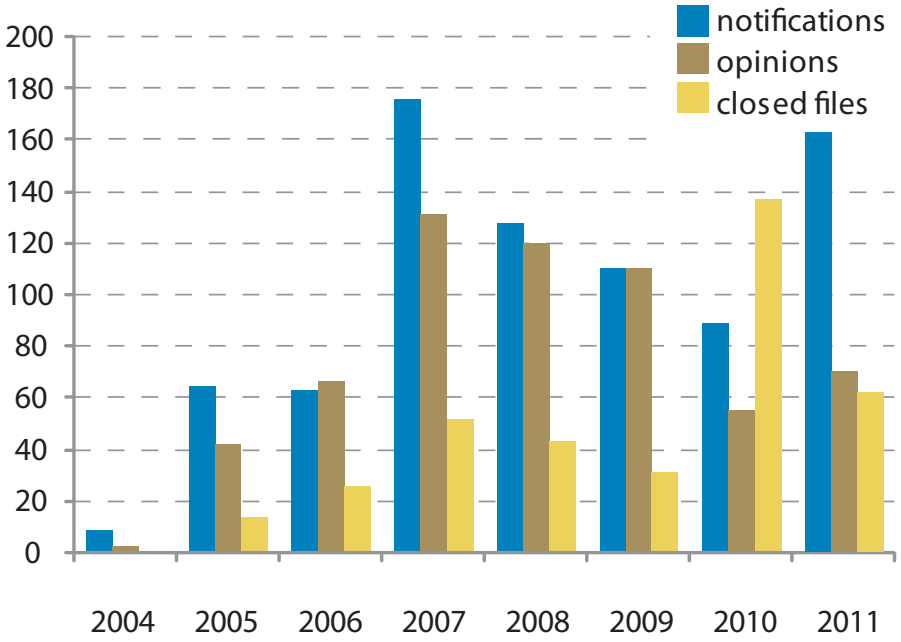
*An EDPS prior check opinion is usually concluded by stating that the processing operation does not violate the Regulation providing certain **recommendations** are implemented. Recommendations are also issued when a case is analysed to decide on the need for prior checking and some critical aspects appear to deserve corrective measures. 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 readily followed the recommendations of the EDPS and to date there has been no need for executive decisions. In the formal letter sent with his opinion, the EDPS requests that the institution or body concerned informs him of the measures taken to implement the recommendations within a period of three months.

The EDPS considers this follow up as a **critical element in achieving full compliance** with the Regulation. In keeping with his 2010 Policy Paper on 'Monitoring and Ensuring Compliance with Regulation (EC) No 45/2001', the EDPS expects institutions and bodies to be **accountable** for any recommendations made. This means that they bear the responsibility for implementing them and they must be able to demonstrate this to the EDPS. Any institution or body failing to act on the recommendations will thus risk formal enforcement action.

2.3.7. Conclusions

Comparative situation



The 71 prior checking opinions issued by the EDPS have provided valuable insight into the processing operations of the European administrations and have enabled the EDPS to build on his expertise in providing generic guidance in certain areas, such as common administrative procedures. This is evident in the processing related to staff evaluation as well as anti-harassment procedures (see section 2.7 on thematic guidelines). The EDPS will continue to provide such guidance to institutions and agencies and continue to facilitate the notification process from the agencies.

Regarding the follow-up of EDPS prior checking opinions, 62 cases were closed in 2011. The EDPS will continue to closely monitor the follow-up work so as to ensure that institutions and agencies integrate recommendations made by the EDPS 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 about an alleged violation of his or her rights related to the protection of his or her personal data. 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 European Union 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 so anonymous requests are not considered as complaints. 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 data. 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 staff member of an EU institution complained about the refusal of access to some data in documents written in the context of a comparative assessment carried out at different stages of the contention procedure related to the decision on merit points. He requested the EDPS to order the institution to provide access to the relevant documents, as they contained his personal data. However, the institution maintained that the document in question never existed. The complainant, therefore, considered that the institution should draft the "missing" documents. The EDPS did not follow the reasoning of the complainant. In fact, the allegation that the institution did not correctly conduct an administrative procedure by not preparing all relevant documents goes beyond the remit of data protection rules. Therefore, no breach of the data protection rules was established in this case.

The processing of personal data 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 citizen of a non-EU country complained to the EDPS about the fact that an entry visa to the Schengen area was refused to him and to his family apparently on the basis of the information provided by the Schengen Information System (SIS). The complainant asked the EDPS to provide him access to his own and his family's personal data included in the SIS. However, even if the SIS is established on the basis of EU law, when it comes to the data subject's right of access, the supervision is exercised not by the EDPS but at national level by national Data Protection Authorities (DPAs). The complainant was therefore advised, that under the current Schengen Agreement, he can request assistance from the national DPA of his choice.

2.4.2. Procedure for handling of complaints

The EDPS handles complaints according to the existing legal framework, the general principles of EU law and good administrative practices common to the EU institutions and bodies. In December 2009, the EDPS adopted an **internal manual** designed to provide guidance to staff when handling complaints. This manual was updated in September 2011 in order to

reflect changes in the organisational structure of the EDPS and to integrate recent developments in the practice of complaint handling. The EDPS has also implemented a **statistical tool** designed to monitor complaint-related activities, in particular to monitor the progress of specific cases.

In all phases of handling a complaint, the EDPS adheres to the principles of proportionality and reasonableness. Guided by the principles of transparency and non-discrimination, he undertakes 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, the EDPS enhanced the process of submitting complaints by providing an interactive **online complaint submission form** on the EDPS website. A provisional version of such a form has been available on the EDPS website since early 2010. This form helps complainants to assess the admissibility of their complaint and thereby submit only relevant matters to the EDPS. It also allows the EDPS to obtain 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 during the final trimester of 2011 by about 60%.

Each complaint received by the EDPS 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.

A complaint for which the EDPS **lacks legal competence** is declared inadmissible and the complainant informed accordingly. In such cases, if relevant, the EDPS informs 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 staff member sent to the EDPS a large number of documents exchanged with an institution that employed him and requested the EDPS to examine them all in order to verify if the data protection rules were respected. The complainant did not formulate any specific allegation of breach of data protection rules nor did he provide the EDPS with any indication or suspicion of such a breach. The EDPS took the position that the complaint does not concern a real or potential breach of data protection rules and decided to close the case without any further inquiry.

A complaint that addresses facts which are **manifestly insignificant**, or would require **disproportionate efforts** to investigate is not pursued. The EDPS 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 data. This includes a study of alternative options to deal with the relevant issue, either by the complainant or by the EDPS. For instance, the EDPS can open an inquiry into a general problem on his own initiative as well as open an investigation into an individual case submitted by a complainant. In such cases the complainant is informed about all available means of action.

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

If the matter is already being examined by administrative bodies – e.g. an internal inquiry by the institution concerned is in progress - the complaint is

admissible in principle. However, the EDPS can decide, on the basis of the particular facts of the case, to await the outcome of those administrative procedures before starting investigations. 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 in November 2006. The MoU stipulates, among other things, that a complaint that has already been examined should not be reopened by another institution unless significant new evidence is submitted.

With regard to **time limits**, if the facts addressed to the EDPS are submitted after a period of two years, the complaint is in principle inadmissible. The two year period starts from the date on which the complainant had knowledge of the facts.

Where a complaint is admissible, the EDPS 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 data and to all information necessary for the inquiry from the institution or body concerned. He 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 data. 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** by the EDPS of his decision within one month of the decision being made. Concerned parties may also appeal directly to the Court of Justice.

No decisions of the EDPS were challenged by complainants in 2011.

On one occasion in 2011, the data controller concerned challenged the decision of the EDPS in the General Court (case T-345/11). The application was rejected by the Court on procedural grounds. The substance of the case was not discussed by the Court.

2.4.3. Confidentiality guaranteed to the complainants

*The EDPS recognises that some complainants put their 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 not disclosed to persons outside the EDPS. However, for the proper conduct of the investigation it may be necessary to inform the relevant services of the institution concerned and the third parties involved about the content of the complaint and the identity of the complainant. The EDPS also copies the Data Protection Officer (DPO) of the institution concerned in all correspondence between the EDPS 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. The EDPS then analyses the complainant's arguments and examines the consequences for the viability of the subsequent EDPS inquiry. If the EDPS decides not to accept the anonymity of the complainant, he explains his evaluation and asks the complainant whether he accepts that the EDPS examines the complaint without guaranteeing anonymity or whether he prefers to withdraw the complaint. If the complainant decides to withdraw the complaint, the institution concerned will not be informed about the existence of the complaint. In such a case, the EDPS may undertake other actions on the matter, without revealing to the institution concerned the existence of the complaint i.e. an inquiry on his own initiative or a request for notification about a data processing operation.

Confidentiality and anonymity are guaranteed by the EDPS to complainants and informants who request it.

At the end of an inquiry, all **documents related to the complaint**, including the final decision remain confidential in principle. They are not published in full nor transferred to third parties. However, an anonymous summary of the complaint can be published on the EDPS website and in the EDPS Annual Report, in a form which does not allow the complainant or third parties to be identified. The EDPS can also decide to publish the final decision *in-extenso* in important cases. This must be done in a way that takes into account a complainant's request for confidentiality and, therefore, does not allow the complainant or other relevant persons to be identified.

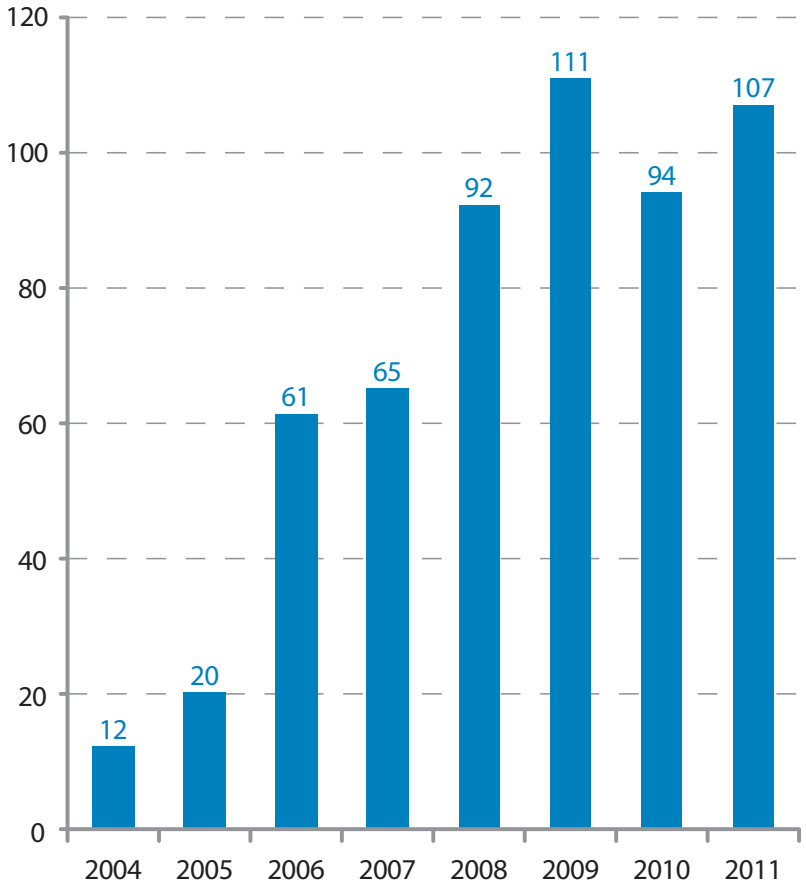
2.4.4. Complaints dealt with during 2011

2.4.4.1. Number of complaints

The number and complexity of complaints received by the EDPS increased in 2011. **In 2011, the EDPS received 107 complaints** (an increase of 14% compared to 2010). Of these, **81 complaints were inadmissible**, the majority relating to processing at national level as opposed to processing by an EU institution or body.

The remaining 26 complaints required more in-depth inquiries (an increase of 4% compared to 2010). In addition, nine admissible complaints, submitted in previous years (one in 2008, five in 2009 and three in 2010), were still in the inquiry, review or follow-up phase on 31 December 2011.

Number of complaints received

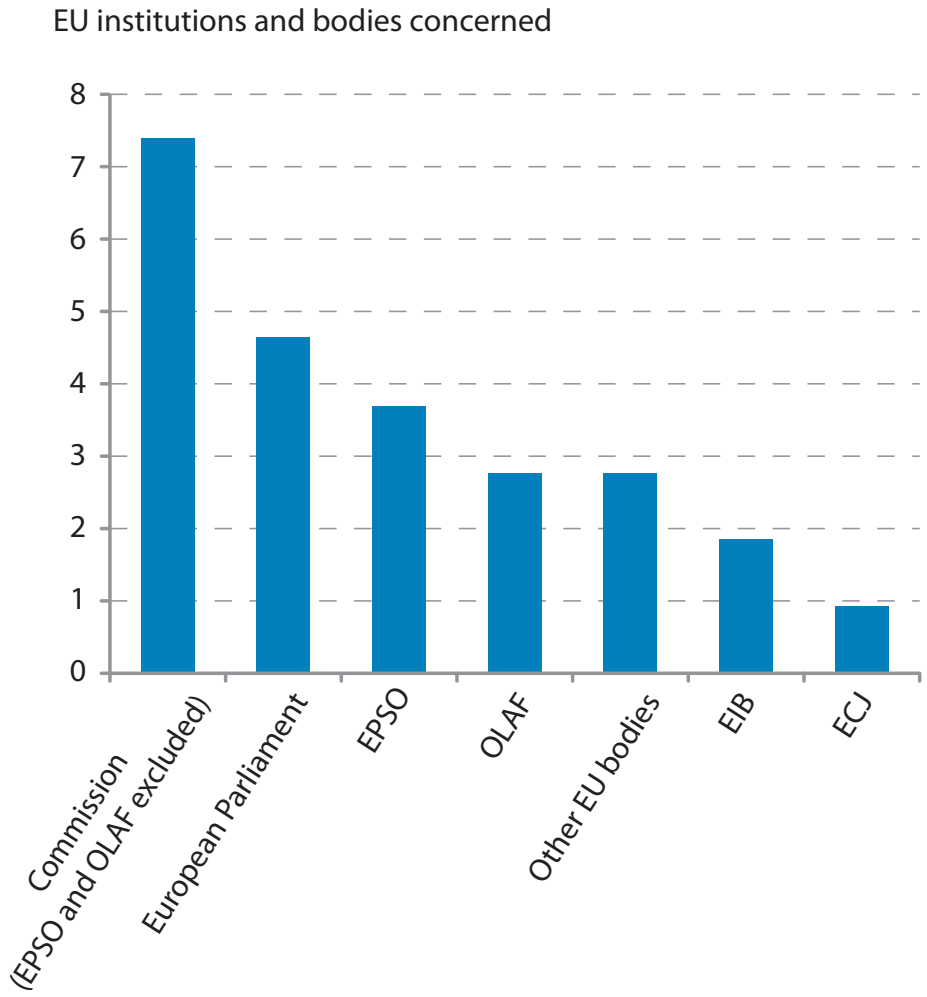


2.4.4.2. Nature of complainants

Of the 107 complaints received, 19 complaints (18%) were submitted by members of staff of EU institutions or bodies, including former staff members and candidates for employment. For the remaining 88 complaints, the complainant did not appear to have an employment relationship with the EU administration.

2.4.4.3. Institutions concerned by complaints

Of the 26 admissible complaints submitted in 2011, most were directed against the **European Commission,** the **European Parliament, OLAF and EPSO**. This is to be expected since the Commission and the Parliament conduct more processing of personal data 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.



2.4.4.4. Language of complaints

The majority of complaints were submitted in English (57%), French (20%) or German (15%). Complaints in other languages are relatively rare (8%).

2.4.4.5. Types of violations alleged

The violations of data protection rules alleged by the complainants in 2011 mainly related to:

- A breach of data subjects' rights, such as access to and rectification of data (30%) or objection and deletion (13%);
- Violation of confidentiality (30%), excessive collection of personal data (17%), loss of data (9%).

Types of violations alleged

2.4.4.6. Results of EDPS inquiries

In 15 cases resolved during 2011, the EDPS found there was no breach of data protection rules or that the necessary measures were taken by the data controller during the EDPS inquiry.

The EDPS received a complaint relating to the transfer, in the context of the departure of an official to another institution, of the number of days of medical absence during the past three years. The EDPS confirmed that such a transfer is in fact necessary for the institution to which the official arrives to fulfil its obligations under Article 59.4 of the Staff Regulations. The EDPS, therefore, concluded in this case that there was no breach of data protection rules.

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

A complaint was received that some documents containing highly sensitive personal data of the complainant and of other persons were available to all staff on the server of an EU body for several weeks. Access to these documents was restricted by the data controller only after the intervention of the complainant. Following an inquiry into the matter, the EDPS concluded that the unauthorised disclosure of the personal data contained in the relevant documents constituted a violation of Article 22 the Regulation (EC) No 45/2001. In order to limit the risk of such a situation arising again in future, the EDPS recommended that the data controller implement a comprehensive system of access rights to different parts of the server.

In one case, non-compliance with data protection rules was found to have occurred without a breach of these rules by the data controller.

A complaint was received from a candidate in an EPSO competition relating to the communication of a document containing sensitive personal data from the selection board of the competition to a person external to the competition. Following an inquiry the EDPS considered that the relevant data controller took reasonable measures to prevent such an unauthorised disclosure, in particular ensuring that all the members of the selection board sign a declaration informing them explicitly of their confidentiality obligations. The EDPS concluded that the disclosure of personal data was illegal and due to an individual action of a specific member of the selection board. The EDPS invited the Appointing Authority to consider a disciplinary procedure against the relevant member of the selection board.

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, targeted monitoring*** *exercises were carried out in cases where, as a result of his supervision activities, the EDPS had cause for concern about the level of compliance in specific institutions or bodies. Some of these were* ***correspondence-based*** *whilst others 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: 2011 Survey

In his policy paper adopted in December 2010([6]), 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*".

In April 2011, the EDPS embarked on his third general stock taking exercise. The exercise had a wide scope, involving six EU institutions and 52 EU bodies and focused on aspects that give a good indication of the progress made in the implementation of the Regulation by institutions and bodies. The conclusions of this exercise were compiled in a report.

The analysis and the report were based on the responses received by September 2011 from EU institutions and bodies (including former second and third pillar bodies) to EDPS letters raising specific questions. The content of the EDPS letters varied slightly according to the status of the institutions and bodies, i.e., young or mature, with or without an appointed Data Protection Officer (DPO).

The responses were displayed in comparative tables, by groups of institutions and bodies. **Benchmarks** were established on the basis of the results of each group to give an indication of the threshold which an institution or body of the relevant group should reasonably be expected to meet. These benchmarks were set up *in concreto* by the EDPS, deduced from the facts, to allow **comparison between peers.**

As a part of EDPS enforcement policy, this general survey was made public. It emphasised the progress made by institutions and bodies and also higlighted the shortcomings in terms of compliance.

The conclusions of this exercise will be taken into account by the EDPS in planning further supervision and enforcement activities. This programme will combine **guidance** to institutions and bodies, **enforcement actions** and measures to promote **accountability**. In particular, compliance visits triggered by a manifest lack of commitment by an institution or body have been planned on the basis of the results of the 2011 exercise.

2.5.2. Targeted monitoring

Pre-recruitment examination by the Parliament's medical service (case 2010-0279)

In the course of 2010, a number of MEPs raised questions as to the appropriate use of the medical questionnaire in the case of parliamentary accredited assistants in the context of the pre-recruitment examination. On 17 March 2011, the EDPS carried out an investigation with the objective to obtain information about the practices of the Parliament's medical service on this issue.

After analysis of the information collected in the course of the inquiry, the EDPS recommended that the medical service of the Parliament clearly communicate to the accredited assistants:

- the status of the medical questionnaire, namely that all the questions are considered necessary and relevant in principle and that in the event that a person wishes not to reply to certain questions, the doctors will assess empirically and on the basis of the medical examination which information is or is not relevant, and

- the consequences of not replying to the questions which the doctors consider necessary and of refusing to present themselves to the pre-recruitment examination.

Secondly, the EDPS recommended that the medical service establish a documented policy for all actors in the medical service on the collection of data in the context of the pre-recruitment examination.

([6]) See the EDPS Policy Paper of 13 December 2010 on "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001", p.8.

In the context of the follow-up, the EDPS considered the case closed, as long as the Parliament officially communicates the documented policy to all actors of its medical service and ensures that they rigorously apply this guidance.

Visits to several Agencies

Between January and September 2011, as a result of a number of issues identified in the course of the 2009 stock taking exercise and its follow up, the EDPS visited several EU agencies in order to discuss and better understand their low level of compliance with the Data Protection Regulation, notably the European Railway Agency, the Community Plant Variety Office, the European Foundation for the Improvement of Living and Working Conditions and the European Global Navigation Satellite Systems Agency.

The visits had a similar structure:

- a meeting between the Supervisor or Assistant Supervisor and the Director of the Agency
- further meetings involving the data protection officer and controllers of processing operations
- presentations on the data protection Regulation and the EDPS approach to monitoring and ensuring regulatory compliance.

These meetings provided an opportunity for the EDPS to raise specific concerns and allowed the Agencies to provide updates on their progress towards compliance.

At the end of each visit, a specific roadmap was agreed upon, detailing priority actions to be undertaken by the Agencies, monitored by the EDPS, in order to ensure a better level of compliance with the Regulation. In general, a good effort has been made by the agencies visited. Bodies that had a rate of Article 25 notifications close to 0 now reach a level of 60, 70, 80 and in one case 100 %. Each body now also has a good, intelligible inventory.

2.5.3. Inspections

Inspections are a crucial tool enabling the EDPS to monitor and ensure the application of the Regulation. They are based on Articles 41(2), 46(c) and 47(2) thereof.

The extensive powers of the EDPS to access any information and personal data necessary for his inquiries and to obtain access to any premises where the controller or the EU institution or body carries out its activity are designed to ensure that the EDPS has sufficient tools to perform his function.

Inspections can be triggered by a complaint or be carried out on 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 inspections, the EDPS **verifies facts on the spot** with the further goal of ensuring compliance. Inspections are followed by appropriate feedback to the inspected institution or body.

In 2011, the EDPS continued the follow-up of previous inspections. In May 2011, the EDPS carried out an inspection at the CEDEFOP and at OLAF. Targeted inspections following a complaint were also carried out by the EDPS at the ECB in October 2011 and at OLAF in December 2011.

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

Following its on-the-spot inspection at the Joint Research Centre in Ispra at the end of 2010, the EDPS adopted an inspection report covering the selection and recruitment of JRC personnel and the different procedures put in place by the security service (pre-employment security check, security investigations, access control and recording of emergency calls).

In 2011, the JRC took a number of steps with a view to bringing its processing operations in line with the data protection regulation, based on the inspection report adopted by the EDPS. Further steps in ensuring compliance still require additional efforts by the JRC. The EDPS expects to conclude this exercise in 2012.

Inspections are a fundamental tool for the EDPS as a supervisory authority.

Inspection at the CEDEFOP

The EDPS conducted an on-the-spot inspection at the European Centre for the Development of Vocational Training (CEDEFOP) in Thessaloniki on 31 May and 1 June 2011. This inspection was part of the EDPS 2011 annual inspection plan, based on an internal risk assessment exercise. Three main areas were inspected: staff recruitment procedures with a focus on current and future practices, access control to the premises managed by the security services and the registry and inventory of notifications.

The background information for the inspection was a combination of prior checking cases and an analysis of consultation cases. Based on its findings, the EDPS drafted an inspection report compiling recommendations with a view to ensuring better compliance with the EU Data Protection Regulation. The CEDEFOP followed-up the inspection report and submitted corrective measures and comments regarding the recommendations of the EDPS. This case should be closed during the first quarter of 2012.

Inspection at OLAF

On 14 and 15 July 2011, the EDPS conducted an on-site inspection at OLAF premises. This inspection was initiated on the basis of Article 47(2) of the Regulation, as a follow-up of several EDPS opinions concerning OLAF external and internal investigations in addition to OLAF physical and logical access control. The investigation particularly focused on how the identification of data subjects is done, how compliance with the obligation to inform data subjects is achieved and how compliance with the data protection obligations on transfers is ensured. A final inspection report was adopted on 12 October 2011, in which the EDPS provided a number of recommendations on which OLAF is expected to comment by early 2012.

Inspection at the European Central Bank

In October 2011, the EDPS conducted an inspection at the European Central Bank (ECB). This inspection took place within the framework of an inquiry into the protection of personal data during internal administrative inquiries. The inspection consisted of an on-the-spot verification of several files related to internal inquiries in which the ECB accessed the electronic files or traffic data. Following the inspection, a number of additional questions relating to the application of the ECB Administrative Circular 01/2006 on internal administrative inquiries and its principles were sent to the ECB. The inquiry has not yet been concluded.

Targeted inspection at OLAF

In October 2009, two complaints were lodged with the EDPS against OLAF concerning the collection and further processing of personal data in the context of an external investigation into the company where the complainants were employed. After careful analysis of the complaints and the relevant responses by OLAF, the EDPS decided to conduct an on-the-spot visit to OLAF's premises in December 2011. The purpose of the visit was to clarify issues related to the proportionality of the collection of digital evidence including personal data by OLAF, using forensic tools (e.g. copying or seizure of hard disk drives).

The visit aimed to assess the overall procedure with regard to the collection and further processing of digital evidence before, during and after an OLAF external investigation and included access to relevant material in OLAF's forensic lab. The information obtained during the visit will be used to finalise the EDPS decision on the above-mentioned complaints.

Visa Information System

The Visa Information System (VIS) allows the exchange of data on short-stay visas among Member States within the Schengen area. It was established by Council Decision 2004/512/EC of 8 June 2004 and the Regulation 767/2008 of the European Parliament and of the Council of 9 July 2008 and allows the competent authorities of the Member States to exchange data on visa applications and on visas issued, refused, annulled, revoked or extended. Biometric data is processed as part of the operation of the VIS.

Regulation 767/2008 provides for coordinated supervision between national data protection authorities and the EDPS. In particular, it provides that the EDPS shall perform an audit of the data processing activities carried out in the central unit and the communication infrastructure every four years. In order to accomplish this task, two on-the-spot visits were carried out by the EDPS, one in July and one in November 2011. The timing of the visits was chosen in order to provide some guidance prior to the system going-live and verify the security measures put in place. The visit in November thus gave the EDPS a baseline against which to compare future inspections.

2.6. Consultations on administrative measures

2.6.1. Consultations Articles 28.1 and 46(d)

*Regulation (EC) No 45/2001 provides for the right of the EDPS to be informed about administrative measures which relate to the processing of personal data (Article 28(1)). The EDPS may issue an opinion, either following a **request** from the institution or body concerned or on his **own initiative**.*

The term 'administrative measure' is to be understood as a decision of the administration of general application relating to the processing of personal data carried out by the institution or body concerned (e.g. implementing measures of the Regulation or general internal rules and policies, as well as decisions adopted by the administration relating to the processing of personal data).

Furthermore, Article 46(d) of the Regulation provides wide material scope for consultations, extending it to 'all matters concerning the processing of personal data'. This is the basis for the EDPS to advise institutions and bodies on specific cases involving processing activities or abstract questions on the interpretation of the Regulation.

Within the framework of consultations on administrative measures envisaged by an institution or body, a variety of issues were examined in 2011, some of which are reported below.

2.6.1.1. Publication of employees' pictures on the Intranet

The "Who is who" project of the Committee of the Regions included the display of a photo of the Committee's staff members with their functions and responsibilities on the Intranet. For this purpose, the Secretary General intended to send an Outlook message to the staff informing them about the project and of the **possibility to opt-out** of having their photo published by clicking on a specific "No, I don't want my picture to be published" tab.

In his reply to the consultation, the EDPS highlighted that "**unambiguous consent**" under Article 5(d) of the Regulation implies that there should be no doubt in every individual case that the data subject freely consents. The proposed system left room for uncertainty as to whether - by taking no action - the staff member really intended to have his/her picture published. Data subjects must be in a position to fully appreciate that they are consenting and what they are consenting to. The most appropriate system to be used to obtain consent is therefore an **opt-in mechanism** requiring an affirmative action to indicate the consent of each staff member before publishing his/her photo.

Consequently, the EDPS recommended that staff members should be provided the option to express consent by clicking on a box stating, for example, "Yes, I want my picture to be published". The EDPS also recommended that the Committee highlight to staff members that they are completely free to give or refuse their consent.

2.6.1.2. Role of an agency in a research project (notion of controllership)

The European Medicines Agency (EMA) consulted the EDPS on certain legal issues raised by its participation in the conduct of a clinical study in the framework of a European-wide research project. The project is carried out by a consortium of 29 members, to which EMA contributes as coordinator.

In particular, the Data Protection Officer of the Agency asked whether EMA could be considered as a **"joint controller"** together with all other participants in the research project and whether the processing of personal data for the clinical study would fall under the scope of the Regulation. On 21 March 2011, the EDPS adopted an opinion highlighting the following aspects of "controllership":

- although EMA specified that the purposes and means of the processing are determined by a steering committee, the EDPS considered that, in this case, **the notion of controller should be analysed with regard to the consortium as a whole;**

- the EDPS considered that all members of the consortium co-decide the conduct of the study. The EDPS was not in a position to evaluate specifically the degree to which members of the consortium – separately or as a whole - control the processing. The EDPS analysis was focused on the responsibilities of EMA, which must be considered one of the controllers.

2.6.1.3. CCTV operated on the premises of another institution

The Trans-European Transport Network Executive Agency (TEN-T EA) consulted the EDPS on the question of the controller-processor relationship where an Agency's CCTV system is operated by another institution. The Agency's video surveillance system is designed, installed, operated and managed by the Commission, based on a 'Service Level Agreement'.

The EDPS replied on 28 July 2011, recalling Opinion 1/2010 of Article 29 Data Protection Working Party on the concepts of 'controller' and 'processor', stressing that the concept of **controller is a functional concept**, intended to allocate responsibilities according to the factual influence. He specified that, in case of doubt, elements such as the degree of actual control exercised by a party, the image given to data subjects and the reasonable expectations of data subjects on the basis of this visibility may be useful to determine the controller.

Based on the facts, the role of the Commission appeared to be more than a mere processor and its role was better described as that of a controller. However, the EDPS pointed out that the Agency could not escape its liability as controller on the grounds that it was obliged to conclude a contract with the Commission whose services are standard and offered to all its partners.

The Agency should exercise due diligence in reviewing the relevant practices of the Commission, communicate Commission practices to its staff and visitors and raise with the Commission (and ultimately, with the EDPS, if legality is at stake) any concerns it may have regarding the legality or customisation of the Commission services as necessary.

Closed circuit television (CCTV) must be used responsibly and with effective safeguards in place.

2.6.1.4. Processing of data in employee emails

The Court of Justice of the European Union (CJEU) consulted the EDPS on some general questions regarding the data processing involved in providing email access to employees. The EDPS replied on 2 September 2011, highlighting the following issues:

- providing email access to employees constitutes the **processing of personal data** under the Regulation, an employer must respect its legal requirements as well as the principle of confidentiality of communications stipulated in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in Article 7 of the Charter of Fundamental Rights of the EU;

- although a particular department (for instance, the IT unit) might be specifically designated as primarily responsible and the contact point for this processing, the CJEU will ultimately be considered the **controller** of the processing;

- it is the controller's responsibility to define the modalities applicable to the processing of personal data in the context of email usage and to **transparently communicate** these modalities to the users. The EDPS recommends adopting **"rules governing the use of emails"** which define the purpose and modalities of the processing. It is up to the controller to ensure that the processing is necessary and that the measures adopted in line with this purpose are proportionate. The rules must be brought to the attention of all users following a possible consultation of staff representatives.

Such rules governing the use of emails should define in particular:

- the **purpose(s) of the processing** of personal data involved in the use of emails. The purpose must be a legitimate one (e.g. ensuring the functioning and security of an email system, but not control the use made of the system in a particular case);

- the modalities applicable to the **private use of emails** (e.g. by obliging the user to clearly indicate the private nature of correspondence in the subject line or in the archiving folder);

- the **retention period(s)** applicable to the messages and security copies in the system, in keeping with the proportionality principle. It is also advisable to specify the period after which the email messages are definitively erased from the server;

Use of emails involves data processing.

- the different types of **security measures** put in place;

- the **access rights** established for IT staff to ensure the proper functioning of the email system;

- the **monitoring measures** put in place by the controller, which must be proportionate to the purpose of the processing and transparent for the users (no silent monitoring of email use). In this context, attention was drawn to the guidance provided in the Working document on the surveillance of electronic communications in the workplace published by the Article 29 Working Party([7]).

2.6.1.5. Using statistical data in a database for staff evaluation purposes

The European Railway Agency (ERA) consulted the EDPS on its intention to use **statistical data on the number of financial operations validated in the ABAC System** ("Accrual Based ACcounting") for the purpose of evaluating the financial initiating agents. Information on the actual number of transactions validated by each agent is available online in ABAC and can also be retrieved by using Business Object reports.

In his reply of 5 May 2011, the EDPS considered that ERA had failed to demonstrate the necessity of using ABAC data for staff evaluation, in particular in view of the evaluation data already collected within

([7]) available under http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf

Statistics may include personal data.

Career Development Reviews at ERA. Also, none of the existing legal instruments provided for the processing of such data for this purpose. Under Article 6(1) of the Regulation, the processing of data for purposes other than those for which they have been collected has to be expressly permitted by the respective internal rules. Consequently, the use of data collected for accountancy purposes for the purpose of evaluating certain financial agents would need to be explicitly allowed.

The EDPS also requested that a notification for (true) prior checking be submitted in due time before the introduction of this new procedure.

2.7. Data protection guidance

The experience gathered in the application of the Data Protection Regulation has enabled EDPS staff to translate their expertise into generic guidance for institutions and bodies. In 2011, this guidance took the form of training for new DPOs or for controllers or thematic guidelines in the field of staff evaluation and processing of personal data in anti-harassment procedures. The EDPS is currently working on guidelines for absences and leaves, procurement and selection of experts, e-monitoring and data transfers.

2.7.1. Thematic Guidelines

Guidelines on anti-harassment procedures

In February 2011, the EDPS issued guidelines on how to manage the processing of personal data in harassment procedures. The guidelines deal with the informal procedure put in place by the EU institutions and bodies to deal with - but also to prevent - harassment. The selection of confidential counsellors, who play a key role in the procedure, is also touched upon in the document.

The confidentiality expected by the data subject is the cornerstone of the informal procedure. From a data protection point of view, the challenge is to ensure the **confidentiality of the data** while allowing the prevention of harassment cases. The guidelines, therefore, make the distinction between hard data (objective data) that can be structurally transferred to Human Resources under certain circumstances to help the identification of recurrent and multiple cases, and soft data (subjective data) that can never be structurally transferred to preserve the confidential character of the procedure.

In addition, the EDPS insists on the principles of the data subject's right of access and right to be informed. In light of the principle of proportionality, restrictions to these rights apply on a case by case basis.

The guidelines are to be used by the agencies in their notification of procedures in this field to the EDPS for prior checking, but should also serve as a practical guide for all institutions and bodies. The EDPS issued a joint opinion on 21 October 2011 on notifications submitted by nine agencies for prior checking in the light of these guidelines.

Guidelines on staff evaluation

In July 2011, the EDPS issued guidelines on the processing of personal data in the area of staff evaluation by EU institutions and bodies.

The objective of the guidelines is to offer practical guidance and assistance to all Data Protection Officers and controllers in their task of notifying existing and/or future data processing operations to the EDPS in the following statutory procedures:

- annual appraisal / career development review (CDR),
- probation,
- promotion of officials,
- re-grading of temporary agents,
- evaluation of the ability to work in a third language before the first promotion,
- re-classification or renewal of a contract for an indefinite period,
- certification of AST officials,
- 'attestation' of former C and D officials.

The DPO network was consulted on the draft guidelines in May 2011 and a presentation of the guidelines was made at the DPO meeting in October 2011.

In the guidelines, the EDPS expressed his concern as to the lengthy conservation period of personal data contained in annual evaluation and probation reports, as well as supporting documents relating to other evaluation procedures kept in personnel files. He recommended that time limits exceeding the career of the staff members concerned be reconsidered and suggested a maximum time limit of five years after a given evaluation exercise, as the best practice.

The DPOs were asked to submit any outstanding notifications by 21 October 2011 to the EDPS. To date, 43 notifications from 21 institutions and bodies concerning 57 evaluation procedures were received by the end of December 2011. The EDPS intends to address all relevant evaluation procedures, per EU institution or body, in a joint opinion.

Follow-up Report on Video-Surveillance Guidelines

In March 2010, the EDPS issued **Video-Surveillance Guidelines**([8]) based on the powers conferred on him in Article 47(1)(a) of Regulation 45/2001.

The Follow-up Report, which was compiled over the course of 2011 and published in early 2012, is a systematic and comparative analysis of the status reports received from a total of 42 EU institutions and bodies. In addition to recognising best practices, this report highlights shortcomings in those institutions and bodies lagging behind in their efforts to ensure compliance with the guidelines. Furthermore, it clarifies certain aspects of the guidelines, where questions were raised by bodies in preparing their video-surveillance policy or a need for clarification became apparent through the analysis of the state-of-play reports.

In the report, the EDPS took note of the considerable efforts undertaken by those institutions and bodies who submitted their state-of-play reports in 2011 and was generally reassured that the guidelines contributed to raising the level of awareness and transparency regarding video-surveillance matters within EU institutions and bodies.

However, more than a year after the adoption of the guidelines and nearly two years after having started the consultation process, the EDPS was disappointed to see that the implementation of the guidelines has been put on hold or significantly delayed in several institutions and bodies.

([8]) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf.

2.7.2. Training

On 10 February 2011, the EDPS organised a training session for ENISA staff as a follow-up to the EDPS visit to ENISA in September 2010. The EDPS provided practical guidance on "Selection and recruitment of staff". This theme was chosen because a prior checking follow up was pending and EDPS had already issued thematic guidelines on the topic. The training session was attended by HR staff, the DPO, the Director and the Head of the administration.

On 8 June 2011, the EDPS organised a one day workshop on data protection for Data Protection Officers from all EU institutions and bodies. The aim was to provide basic training for DPOs, particularly for recently-appointed ones. The workshop began with an introduction to the basic principles and definitions of the regulation. This was followed by a session which included presentations on legal issues (e.g. legal basis of data processing, rights of the data subject, transfer of data, processing on behalf of the controller). The afternoon session was dedicated to cooperation between DPOs and the EDPS, focusing on the practical aspects of complaint handling, prior-checking procedures, and security of processing operations.

The workshop was well-attended and active participation of the DPOs led to a productive exchange of experiences and concerns. The EDPS will build on this experience and based on the feedback received, organise a similar workshop for Data Protection Coordinators in 2012.

In November 2011, EDPS staff provided training at the Auditors Forum, a monthly conference addressed to the internal auditors of the European Commission. The presentation covered a general introduction to data protection and compliance with the data protection rules by internal audit services in the performance of their activities. The training was well attended by Commission staff and was also followed by video conference by the internal audit services of the European Court of Auditors, the European Court of Justice and the European Central Bank.

On request from the TEN TEA DPO, EDPS staff provided general training on data protection and the Regulation to TEN TEA staff on 1 December 2011. The first session was dedicated to data protection and the basic principles of the Regulation. This was followed by a presentation on the EDPS enforcement policy and then by a Q&A session. The training was well-attended by TEN TEA staff.

Personal data are processed by EU institutions and bodies during staff evaluation procedures.

3 POLICY AND CONSULTATION

3.1. Introduction: overview of the year and main trends

In 2011, the Commission published many legislative proposals affecting data protection and made significant headway towards a new general and comprehensive framework for data protection in Europe.

The ongoing work on the new data protection legislation framed 2011: on 14 January, the EDPS published his opinion on the Commission Communication on the comprehensive approach to personal data protection in the European Union; in December, he provided informal comments on draft proposals to DG Justice, which is responsible for the new legal framework. On both occasions, the EDPS provided substantive input into the legislative procedure. He will continue to do so in 2012.

This project featured high on the EDPS agenda in 2011 and will remain so for the coming years as the legislative procedure advances: once the Commission has presented its proposal and accompanying communication in 2012, the EDPS will provide an opinion. Thereafter, the discussions in the European Parliament and the Council will proceed.

Following the trend of past years, the areas covered by EDPS opinions continued to diversify. Aside from traditional priorities, such as the further development of the Area of Freedom, Security and Justice or international data transfers, new fields are emerging. 2011 saw a number of opinions issued on matters related to the internal market, as well as fisheries control and agricultural support schemes.

In the **Area of Freedom, Security and Justice**, the question of necessity has been a recurrent theme. On several occasions, the EDPS issued opinions in which this data protection principle figured prominently. This was the case for the evaluation report on the Data Retention Directive, the communication on migration and the proposal for an EU Passenger Name Records Programme.

Necessity is a key concept in data protection. It is a strict rather than simply "useful" standard: A measure can only be considered necessary if the results could not have been achieved with less intrusive means. Especially when evaluating existing measures, this standard must be applied with utmost rigour. This standard of proof is enshrined in European law and has been applied extensively by the Court of Justice of the European Union in Luxembourg as well as by the European Court for Human Rights in Strasbourg, usually closely linked to the standard of proportionality.

Passenger Name Records were also a recurrent topic when the EDPS was consulted on initiatives in the field of international law enforcement and security cooperation. He issued opinions on the proposals for agreements with the USA and Australia.

The increasing number of opinions related to the **internal market** is a new development and among

others, the EDPS adopted opinions on the Internal Market Information System and over-the-counter derivatives.

In another innovation, the EDPS published his first **opinion on EU-funded research activities**, providing advice to European research and development activities. This opinion put the policy paper 'The EDPS and EU Research and Technological Development' into practice.

The wide range of issues addressed in EDPS consultative activities demonstrates that the processing of personal data and data protection have truly become horizontal issues that cannot be confined to specific policy areas. Instead, they are of cross-cutting relevance, justifying the role of the EDPS as the competent adviser to the EU institutions.

This chapter of the Annual Report not only focuses on legislative consultation but also deals with relations between the EDPS and the EU Courts and with the monitoring of new developments by the EDPS, in particular new technologies. Cooperation with DPAs, including coordinated supervision on large scale information systems, is included in Chapter 4.

3.2. Policy framework and priorities

3.2.1. Implementation of consultation policy

Although the working methods of the EDPS in the area of consultation have developed over the years, the basic approach for interventions has not changed. The policy paper adopted in March 2005 and entitled "The EDPS as an advisor to the Community institutions on proposals for legislation and related documents"([9]) remains relevant, although it must now be read in light of the Lisbon Treaty.

The formal opinions of the EDPS - based on Article 28(2) or 41 of Regulation (EC) No 45/2001 - are the main instruments of consultation policy and contain a full analysis of all the data protection related elements of any Commission proposal or other relevant instrument.

([9]) Available on the EDPS website under Publications > Papers.

Legislative consultations based on Article 28(2) of Regulation (EC) No 45/2001 are the core element of the EDPS advisory role. According to this article, the Commission shall consult the EDPS when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms. The EDPS opinions fully analyse the data protection aspects of a proposal or other text.

As a rule, the EDPS only issues 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 convey quickly a fundamental political message or to focus on one or more technical aspects. They are also used to summarise or repeat observations made earlier. For instance, the EDPS wrote two letters on several legislative proposals on restrictive measures, as the data protection issues in these proposals were largely similar to those addressed in earlier opinions.

Other instruments can also be used, such as 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 of the European Parliament or in the relevant working parties in the Council.

The EDPS is available to the EU institutions during all phases of policy making and legislation and uses a wide range of other instruments in his advisory role. Although this may require close contact with the institutions, maintaining his independence remains paramount.

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 applies to long-term projects in particular, such as the reform of the legal framework for OLAF to which the EDPS 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 usually sent to the EDPS during the inter-service consultation, i.e. before it is published. These informal comments, of which there were 41 in 2011, 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, these usually refer to the fact that informal comments have been submitted earlier.

Regular contact with the relevant services of an institution will take place following the issuing of EDPS comments or opinion. In some cases, the EDPS and his staff are closely 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 in 2011

In 2011, the steady increase in the number of opinions issued continued. The EDPS issued 24 opinions, 12 formal comments and 41 informal comments on a variety of subjects.

With these opinions and other instruments used for intervention, the EDPS implemented his priorities for 2011, as laid down in his inventory. The 24 opinions covered different EU policy areas.

The 2011 Inventory defined four main areas of attention:

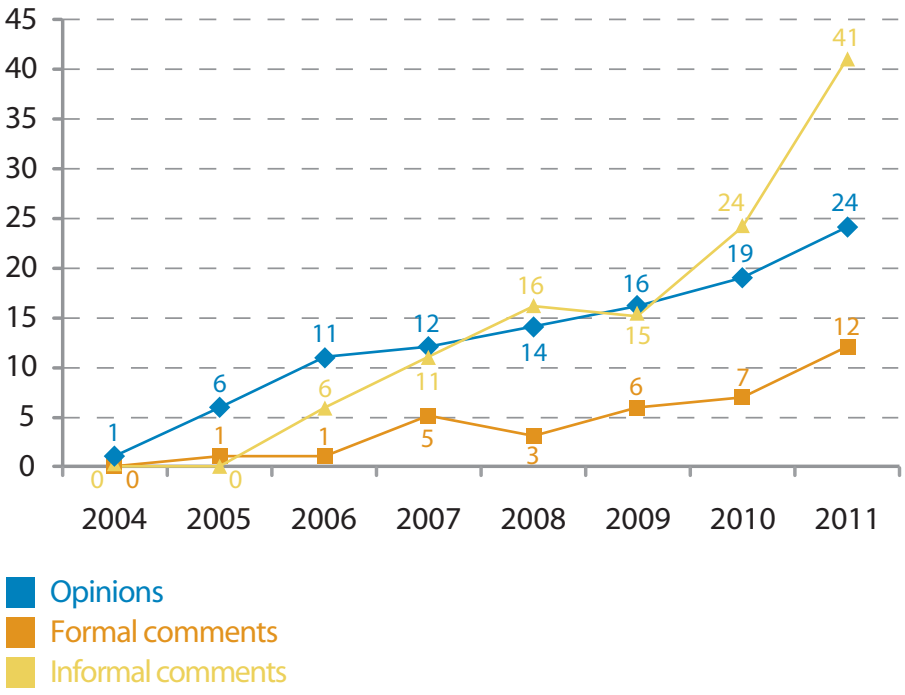
a) towards a new legal framework for data protection

b) further developing the Area of Freedom, Security and Justice

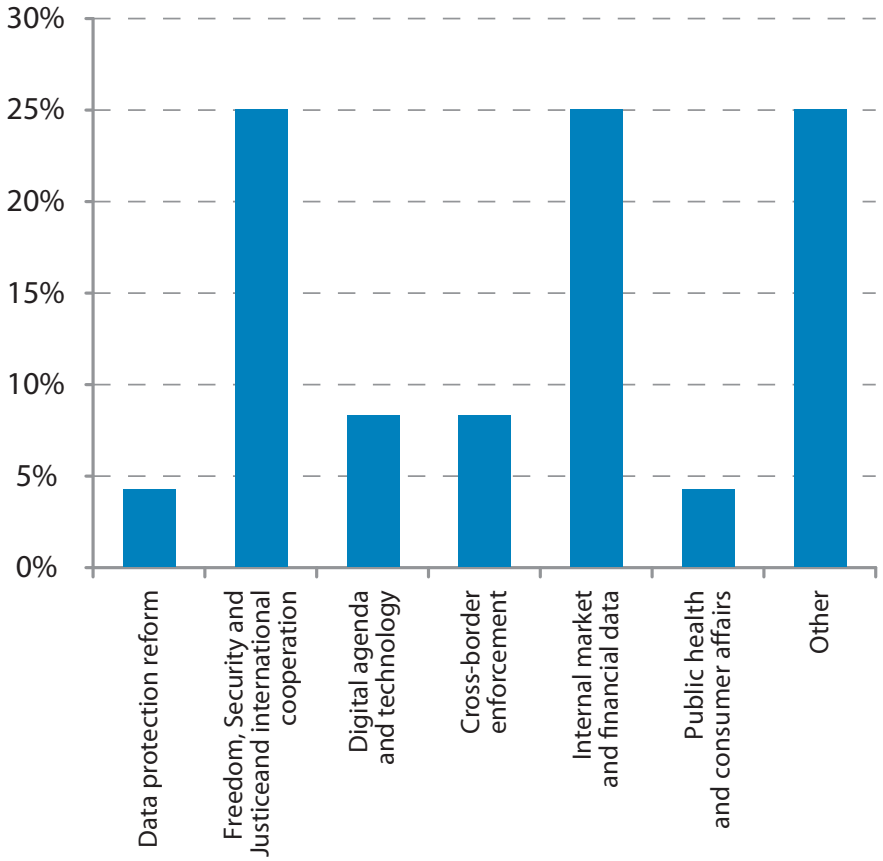
c) technological developments and the Digital Agenda

d) other initiatives with a significant impact on data protection.

Legislative opinions evolution 2004-2011



Main policy areas for legislative opinions in 2011



3.3. Review of the EU Data Protection Framework

3.3.1. A comprehensive approach to personal data protection in the European Union

On 14 January 2011, the EDPS issued an opinion on the Commission Communication on the review of the EU legal framework for data protection. The Communication is an essential landmark on the way towards a new legal framework that will represent the most important development in the area of EU data protection since the adoption of the EU Data Protection Directive 17 years ago.

The EDPS has welcomed the Commission's intention to reform the EU legal framework for data protection - which he has previously requested on a number of occasions([10]) - and the review of the legal framework already was one of the top priorities for the EDPS in 2009 and 2010. He shared the Commission's view that in the future a strong system of data protection is absolutely necessary, based on the notion that the existing general principles of privacy and data protection remain valid.

In his opinion, the EDPS supported the main issues and challenges identified by the Commission, but asked for more ambitious solutions to make the system more effective and give citizens better control over their personal data.

([10]) see e.g.: Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, p. 1

In the EDPS' view, the major goals of the review process should be as follows:

- **the rights of individuals should be strengthened**: the EDPS suggests introducing a mandatory security breach notification covering all relevant sectors, as well as new rights, especially in the online environment, such as the right to be forgotten and data portability. Children's data should also be better protected;
- **the responsibility of organisations needs to be reinforced**: the new framework must contain incentives for data controllers in the public or private sector to proactively include new tools in their business processes to ensure compliance with data protection (accountability principle). The EDPS proposes the introduction of general provisions on accountability and 'privacy by design';
- **the inclusion of police and justice cooperation in the legal framework** is a *conditio sine qua non* for effective data protection in the future;
- **further harmonisation** should be one of the key objectives of the review. The Data Protection Directive should be replaced by a directly applicable regulation;
- the new legal framework must be formulated in a **technologically neutral** way and must have the ambition to create **legal certainty** for a longer period;
- the enforcement powers of **data protection authorities** should be strengthened, and their independence should be better guaranteed across the EU.

The Commission will adopt two legislative proposals in early 2012, one proposal for a general data protection regulation and another one for a directive on data protection in the field of law enforcement. The EDPS will, of course, continue to monitor the legislative process and will issue further contributions as appropriate.

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

3.4.1. Data Retention

Under the Data Retention Directive public electronic communications providers (telephone companies, mobile telecoms and Internet service providers) are obliged to retain traffic, location and subscriber data for the purposes of investigation, detection and prosecution of serious crime.

The EDPS opinion adopted on 31 May 2011 analysed the Commission Report which provides an evaluation of the implementation and application of the Data Retention Directive and measures its impact on economic operators and consumers.

The EDPS took the view that the Directive **does not meet the requirements imposed by the fundamental rights to privacy and data protection** for the following reasons:

- the necessity for data retention provided for in the Directive has not been sufficiently demonstrated;
- data retention could have been regulated in a less privacy-intrusive way;
- the Directive leaves too much scope for Member States to decide on the purposes for which the data might be used and for determining who can access the data and under which conditions.

The EDPS pointed out that information provided by the Member States was not sufficient to draw a positive conclusion on the need for data retention as developed in the Directive. Further investigation of necessity and proportionality is required and in particular, the examination of alternative, less privacy-intrusive means.

The Commission (Evaluation) Report plays a role in possible decisions on amending the Directive. The EDPS has therefore called on the Commission to seriously consider all options in this process, including the possibility of repealing the Directive, whether or not combined with the proposal for an alternative, more targeted EU measure.

Data Retention Directive poses a massive invasion of privacy.

If, on the basis of new information, the necessity for an EU instrument on data retention is demonstrated, the following basic requirements should be respected:

- it should be comprehensive and genuinely harmonise rules on the obligations to retain data, as well as on the access and further use of the data by competent authorities;
- it should be exhaustive, which means that it has a clear and precise purpose which cannot be circumvented;
- it should be proportionate and not go beyond what is necessary.

*The EDPS stressed that the massive invasion of privacy posed by the Data Retention Directive needed profound justification. The EDPS, therefore, called on the European Commission to use the evaluation exercise to **prove the necessity** of the Directive. Concrete facts and figures should make it possible to assess whether the results presented in the evaluation could be achieved by other less intrusive means.*

3.4.2. Terrorist Finance Tracking System (TFTS)

On 25 October 2011, the EDPS sent his comments on the Commission Communication on the Terrorist Finance Tracking System of 13 July 2011 to the Commissioner for Home Affairs. He supported all the points made by the Article 29 Working Party in its letter of 29 September 2011, particularly regarding the principles of necessity and proportionality, data controllers and processor relationships, bulk data transfers, types of data being processed, retention, rights of data subjects, DPAs, data security and cooperation between the Member States. Moreover, he highlighted **necessity and proportionality as the procedural guarantees** that should be introduced into any EU TFTS scheme.

3.4.3. European Passenger Name Records

In 2011, as in previous years, the proposed processing of Passenger Name Records (PNR) by law enforcement authorities raised data protection issues from a European perspective.

On 25 March 2011, the EDPS adopted an opinion which analysed the new Commission proposal obliging airline carriers to provide EU Member States with the personal data of passengers (Passenger

Name Record) entering or departing the EU for the purposes of fighting serious crime and terrorism.

In his opinion, the EDPS recalled that the need to collect or store massive amounts of personal information must rely on a **clear demonstration of the relationship between use and result** (necessity principle). This is an essential prerequisite for any development of a PNR scheme. In the view of the EDPS, the current acts failed to demonstrate the necessity and the proportionality of a system involving large-scale collection of PNR data for the purpose of a systematic assessment of all passengers.

3.4.4. Agreement between the EU and Australia on Passenger Name Records

On 15 July 2011, the EDPS adopted an opinion on a Commission proposal concerning an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data. The EDPS welcomed the safeguards provided in the proposals, especially with regard to the concrete implementation of the agreement, in particular data security aspects, supervision and enforcement provisions.

However, he also identified significant **room for improvement**, in particular as regards the scope of the agreement, the definition of terrorism and the inclusion of some exceptional purposes, as well as the retention period for PNR data. He also considered that the legal basis for the agreement should be reconsidered and should refer to Article 16 of the Treaty on the Functioning of the European Union (TFEU).

In addition, the EDPS recalled the wider context of the **legitimacy** of any PNR scheme, seen as the systematic collection of passenger data for risk assessment purposes. A proposal can satisfy the other requirements of the data protection framework, only if the scheme respects the fundamental requirements of necessity and proportionality under Articles 7 and 8 of the Charter of Fundamental Rights and Article 16 TFEU.

The EDPS recommendations included the following:

- **scope of application**: the scope of application should be much more limited with regard to

Personal information is collected by airlines or travel agencies at the time a passenger makes a reservation, before travelling.

the type of crimes involved. The EDPS recommends explicitly defining and excluding minor crimes from the scope and precluding Member States from expanding the scope;

- **data retention**: no data should be kept beyond 30 days in an identifiable form, except in cases requiring further investigation;
- **data protection principles**: a higher standard of safeguards should be developed, particularly in terms of data subjects' rights and transfers to third countries;
- **list of PNR data**: the EDPS welcomes the fact that sensitive data are not included in the list of data to be collected but still regards the list as too extensive and recommends that it is further reduced;
- **evaluation of EU PNR system**: the assessment of the implementation of the system should be based on comprehensive statistical data, including the number of persons effectively convicted - and not only prosecuted - on the basis of the processing of their personal data.

Finally, the EDPS recalled that the need to collect or store massive amounts of personal information must rely on a clear demonstration of the relationship between use and result (necessity principle). This is an essential prerequisite for any development of a PNR scheme. In the view of the EDPS, the proposal and accompanying impact assessment failed to demonstrate the necessity and the proportionality of a system involving large-scale collection of PNR data for the purpose of a systematic assessment of all passengers.

3.4.5. Agreement between the EU and USA on Passenger Name Records

The EDPS was critical of the new proposal for an EU-US Passenger Name Record (PNR) agreement, as the necessity and the proportionality of PNR schemes have not yet been demonstrated. In his opinion of 9 December 2011, he criticised:

- the **15-years retention period**: the EDPS recommended deleting the data after its analysis or after a maximum of 6 months;
- the **overbroad purpose definition**: the purpose should be limited to combating terrorism or a well defined list of transnational serious crimes;
- the **amount of data to be transferred** to the Department of Homeland Security (DHS): it should be narrowed and exclude sensitive data;
- the **exceptions to the "push" method**: US authorities should not directly access the data ("pull" method);
- the **limits to data subjects' exercising their rights**: every citizen should have the right to effective judicial redress;
- the **rules on onward transfers**: the DHS should not transfer the data to other US authorities or third countries unless they guarantee an equivalent level of protection.

The EDPS considered that neither the main concerns previously expressed by the EDPS and the EU national data protection authorities, nor the conditions required by the European Parliament to provide its consent were met.

3.4.6. Anti-corruption package

On 6 July 2011, the EDPS issued formal comments on the anti-corruption package, which consisted of a communication setting out the European Union's approach to curb corruption, a Commission decision to establish a regular EU anti-corruption report and a report on the terms of EU participation in the Council of Europe Group of States against Corruption.

The communication refers to a planned strategy for improving the quality of financial investigations and developing financial intelligence, including sharing of information within and between Member States, EU agencies and third countries. In this regard, the EDPS encouraged the Commission to **ensure a sufficient level of data protection in this future strategy**. He also recommended that the sharing of best practices envisaged in the EU anti-corruption report should be understood to also include practices for ensuring data protection in anti-corruption investigations.

3.4.7. Legislative proposals concerning certain restrictive measures

On 16 March and 9 December 2011, the EDPS sent letters to the European Commission, the European

Parliament, the Council and the High Representative of the Union for Foreign Affairs and Security Policy as a response to the Commission consultation on various legislative proposals concerning certain restrictive measures with regard to Iran, the Republic of Guinea-Bissau, Côte d'Ivoire, Belarus, Tunisia, Egypt, Libya, Syria, Afghanistan and Burma/Myanmar. In his letters, the EDPS reaffirmed his position that when EU institutions take restrictive measures with regard to individuals, **data protection principles and any necessary restrictions to them should be comprehensively and clearly laid down.**

The Commission proposals envisaged fighting human rights abuses by imposing restrictive measures - notably, freezing of assets and economic resources - on natural and legal persons who are considered to be involved in such abuses. To this end, "blacklists" of the natural or legal persons concerned are published and publicised.

The EDPS criticised that while the text initially proposed by the Commission and the High Representative included strong references to data protection rules, they were significantly weakened by the Council. He reiterated the recommendation to the Commission, the High Representative and the Council to abandon the current piecemeal approach - with specific data protection rules for each country or organisation - and to develop a **consistent framework for restrictive measures**, ensuring respect of fundamental rights and in particular, the fundamental right to the protection of personal data.

3.4.8. Migration

In 2011, the Commission worked on a comprehensive approach to migration. To outline its position and agenda, it published a communication on this topic in May. On 7 July 2011, the EDPS adopted an opinion on this communication.

Use of biometrics should be accompanied by strict safeguards.

In his opinion, the EDPS focused on the **need to prove the necessity of the proposed new instruments** such as the Entry-Exit-System. To this end, he recalled the case law of the European Court of Human Rights and the European Court of Justice, which establishes that the standard of proof needed to interfere with the right to privacy and data protection is that of 'being necessary in a democratic society' and elaborated on the concept of necessity.

Also addressed was the use of biometrics. Here, the EDPS urged that **any use of biometrics should be accompanied by strict safeguards and complemented by a fall-back procedure** for persons whose biometric characteristics may not be readable. Additionally, he specifically **called on the Commission not to reintroduce the proposal to grant law-enforcement access to Eurodac** (a large-scale IT system devoted to storing fingerprints, see 4.2).

By explicitly stating his position on this topic, the EDPS gave guidance to the Commission on how to evaluate necessity. It can be noted that subsequent Commission documents, such as the Communication on smart borders, show increased attention to this concept.

3.4.9. Victims of crime

On 17 October 2011, the EDPS published his opinion on the legislative package on the victims of crime, which focuses on privacy-related aspects of the protection of the victims of crime. The EDPS welcomed the policy objectives of the proposals and generally endorsed the approach of the Commission. Nevertheless, he found that the protection of privacy and personal data of the victims in the proposed directive could have been strengthened and clarified.

With regard to the proposed Regulation on mutual recognition of protection measures in civil matters, which deals with protection of individuals against other individuals causing risks to them ("stalking") the EDPS suggested that information about the protected person **to the person causing the risk should be limited** to those personal data which are strictly necessary for the execution of the measure.

3.5. Digital Agenda and technology

The Commission carried out significant work in the area of the information society and new technologies in 2011. Particular emphasis was given to 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 the EDPS. He also monitored and engaged in relevant European research and technological development projects.

Apart from the initiatives mentioned below, the EDPS also provided advice on additional proposals included in the Digital Agenda action plan, namely the public consultation on the Intellectual Property Rights Enforcement Directive([11]) and the legal framework for the Consumer Protection Cooperation System (CPCS)([12]).

3.5.1. Net neutrality

On 7 October 2011, the EDPS adopted an opinion on the Commission Communication on the open Internet and net neutrality in Europe.

Net neutrality raises many data protection related issues.

The EDPS highlighted the serious **implications** of some monitoring practices of ISPs on the **fundamental right to privacy and data protection of users**, in particular in terms of confidentiality of communications. He has called on the Commission to initiate a debate involving all the relevant stakeholders with a view to **clarifying how the data protection legal framework applies** in this context.

He recommended guidance to be provided in areas such as:

- determining inspection practices that are **legitimate**, such as those needed for security purposes;
- determining when monitoring requires the **users' consent**, for instance in cases where filtering aims to limit access to certain applications and services, such as peer to peer.

In particular the guidance should cover the application of the necessary **data protection safeguards** such as purpose limitation and security.

3.5.2. Technological project "Turbine"

On 1 February 2011, the EDPS adopted an opinion based on his policy paper "The EDPS and EU Research and Technological Development", adopted in 2008. This paper described the possible roles the EDPS could play for research and technological development (RTD) projects in the context of the Commission Framework Programme for Research and Technological Development.

In his opinion, the EDPS analysed the Turbine (TrUsted Revocable Biometric IdeNtitiEs) research project, the overall objectives of which are to:

- develop an innovative, privacy enhancing technology solution for electronic identity (eID) authentication through fingerprint biometrics;
- demonstrate the performance and security of this solution for use in commercial eID management applications, as well as its benefit for the citizen in terms of enhanced privacy protection and user trust in electronic identity management through the use of fingerprints.

The analysis of the EDPS focused on some important features of the project, namely the protection of the biometric template by cryptographic transformation of the fingerprint information into a **non-reversible** key (where it is not possible to return to the original biometric information) and

Turbine - TrUsted Revocable Biometric IdeNtitiEs

([11]) see below Section 3.7.1

([12]) see below Section 3.8.1

the **revocability** of this key (where a new independent key can be generated to re-issue biometric identities). Moreover, through the test phase, the project tested implementation of the features in real case scenarios.

The EDPS welcomed the project as it demonstrates that implementing "privacy by design" as a key principle in research, represents an effective means to ensure "privacy compliant" solutions.

3.6. Internal Market including financial data

3.6.1. Internal Market Information System

In his opinion of 22 November 2011, the EDPS provided a series of recommendations to further strengthen the data protection framework for the Internal Market Information System (IMI). The EDPS supported a consistent approach to data protection in establishing an electronic system for the exchange of information, including relevant personal data.

The EDPS welcomed the fact that the Commission proposed a horizontal legal instrument for IMI in the form of a Parliament and Council Regulation, which aims to comprehensively highlight the most relevant data protection issues for IMI. The EDPS cautioned that there are associated risks in establishing a single centralised electronic system for multiple areas of administrative cooperation. With regard to the legal framework for IMI to be established in the proposed Regulation, the EDPS drew attention to two key challenges: **the need to ensure consistency while respecting diversity** and **the need to balance flexibility and legal certainty**.

The EDPS acknowledged the need for flexibility to cover administrative cooperation in different policy areas but insisted that this flexibility should be accompanied by legal certainty. Against this background, the EDPS recommended that the functionalities of IMI already foreseen should be further clarified and that the inclusion of new functionalities should require appropriate procedural safeguards, such as preparation of a data protection impact assessment and consultation of the EDPS and national data protection authorities.

The opinion also called for further strengthening of data subjects' rights and reconsideration of the extension of the current 6-month retention period unless adequate justification can be provided.

Finally, the EDPS welcomed the provisions on coordinated supervision and recommended that these should be further strengthened in order to guarantee effective and active cooperation among the data protection authorities involved.

3.6.2. Energy Market Integrity and Transparency

On 21 June 2011, the EDPS issued an opinion on the proposal for a regulation on energy market integrity and transparency. The main aim of the proposal is to prevent market manipulation and insider trading on wholesale energy - gas and electricity - markets. The EDPS commented on several aspects of the proposal, including those on market monitoring and reporting and investigation and enforcement.

The key concern of the EDPS was that the proposal **lacked clarity and adequate data protection safeguards** with regard to the investigatory powers granted to national regulatory authorities. The EDPS, therefore, recommended clarification on:

The EDPS took a close look at the proposal for a regulation on the energy market.

- whether **on-site inspections** would be limited to business properties or also apply to private properties of individuals. In the latter case, the necessity and proportionality of this power should be clearly justified and a judicial warrant and additional safeguards required;

- the **scope of the powers** to request "existing telephone and existing data traffic records". The proposal should unambiguously specify what **records** can be requested and from whom. The fact that no data can be requested from providers of publicly available electronic communications services should be explicitly mentioned. The proposed regulation should clarify whether the authorities may also request the private records of individuals (e.g. text messages sent from personal mobile devices). If this were the case, the necessity and proportionality of this power should be clearly justified and the proposal would also require a warrant from a judicial authority.

The reporting and collection of data regarding suspicious transactions was another sensitive subject in the proposal where the EDPS called for the clarification of the relevant provisions and adequate safeguards, such as strict purpose limitations and retention periods.

3.6.3. Interconnection of business registers

On 6 May 2011, the EDPS issued an opinion on the proposal for a directive amending three existing directives on the interconnection of business registers. The aim of the proposal is to facilitate and step up cross border cooperation and information exchange among business registers in the European Union, thereby increasing transparency as well as reliability of the information available across borders.

The main concern of the EDPS is that the proposal, as drafted, would leave key issues such as those of governance, roles, competences and responsibilities to delegated acts. In order to **ensure legal certainty** as to who is responsible for what and to ensure that adequate data protection safeguards can be identified and implemented, the EDPS recommended that these key issues be addressed in the proposed directive.

3.6.4. Credit agreements relating to residential property

On 25 July 2011, the EDPS adopted an opinion on a Commission proposal for a directive on credit agreements relating to residential property. Responsible lending is defined by the proposal as the care taken by creditors and intermediaries to lend amounts that consumers can afford and meet their needs and circumstances. The proposal was drafted from the perspective that irresponsible behaviour by some market players was at the source of the financial crisis. The proposal, therefore, introduces prudential and supervisory requirements for lenders and obligations and rights for borrowers in order to establish a clear legal framework that should safeguard the EU mortgage market from the disruptive effects experienced during the financial crisis.

The EDPS welcomed the specific reference in the proposal to Directive 95/46/EC. However, he suggested some modifications to the text in order to clarify the **applicability of the data protection principles to the processing operations**, particularly in relation to the consultation of the database on credit-worthiness which is established in almost all Member States.

Credit agreements are a subject to applicability of the data protection principles.

3.6.5. Over-the-counter derivatives, central counterparties and trade repositories

The opinion, published by the EDPS on 19 April 2011, focused primarily on the specific investigation powers granted to the European Securities and Markets Authority (ESMA) under the proposed Regulation, namely the power to "**require records of telephone and data traffic**".

*The opinion highlights that investigatory powers directly relating to traffic data, given their potential intrusiveness, have to comply with the requirements of **necessity and proportionality**. It is, therefore, essential that they are clearly formulated in their personal and material scope, as well as the circumstances and conditions in which they can be used. Adequate safeguards should also be provided against the risk of abuse.*

The EDPS considered that these requirements were not fulfilled in the proposed Regulation as the power under consideration was **too broadly formulated**. In particular, the **personal and material scope** of the power, the **circumstances and the conditions** under which it could be used were not specified. The EDPS, therefore, called for more clarity and advised the legislator to:

- clearly specify the categories of telephone and data traffic records which trade repositories are required to retain and/or to provide to the competent authorities;
- limit the power to require records of telephone and data traffic to trade repositories only;
- state explicitly that accessing telephone and data traffic records directly from telecom companies is excluded.

The EDPS also recommended limiting the exercise of the power to **identified and serious violations** of the proposed Regulation and in cases where a **reasonable suspicion** of a breach exists. Furthermore, he suggested that prior **judicial authorisation** (at least where such authorisation is required under national law) and adequate procedural safeguards against the risk of abuse be introduced.

3.6.6. Technical requirements for credit transfers and direct debits in Euros

On 23 June 2011, the EDPS adopted an opinion on a Commission proposal for a Regulation establishing technical requirements for credit transfers and direct debits in Euros, which relates to the Single European Payment Area (SEPA).

Introduction and development of SEPA involve several data processing operations.

The SEPA project aims to establish a single market for retail euro payments by overcoming the technical, legal and market barriers that exist prior to the introduction of the single EURO currency. Once SEPA has been completed, there will be no difference between national and cross border Euro payments.

The introduction and development of SEPA involves several data processing operations: names, bank account numbers and content of contracts need to be exchanged directly between payers and payees and indirectly through their respective payment service providers in order to guarantee a smooth functioning of the transfers. The proposal also introduces a new role for national authorities competent to monitor compliance with the Regulation and take all necessary measures to ensure such compliance. While this role is fundamental for guaranteeing an effective implementation of SEPA, it might also involve broad powers for the further processing of personal data by the authorities, including the total amount of Euro transfers between individuals and entities.

The EDPS, therefore, recommended some modifications to the text in order to **ensure that exchanges of such data comply with the relevant applicable legislation**, particularly with the principles of necessity, proportionality and purpose limitation.

3.6.7. Airport body scanners

On 17 October 2011, the EDPS sent a letter to the European Commission Vice-president Sim Kallas concerning three proposals on common basic standards on civil aviation security as regards the use of security scanners at EU airports. The draft measures were adopted by the Commission using the "comitology" procedure.

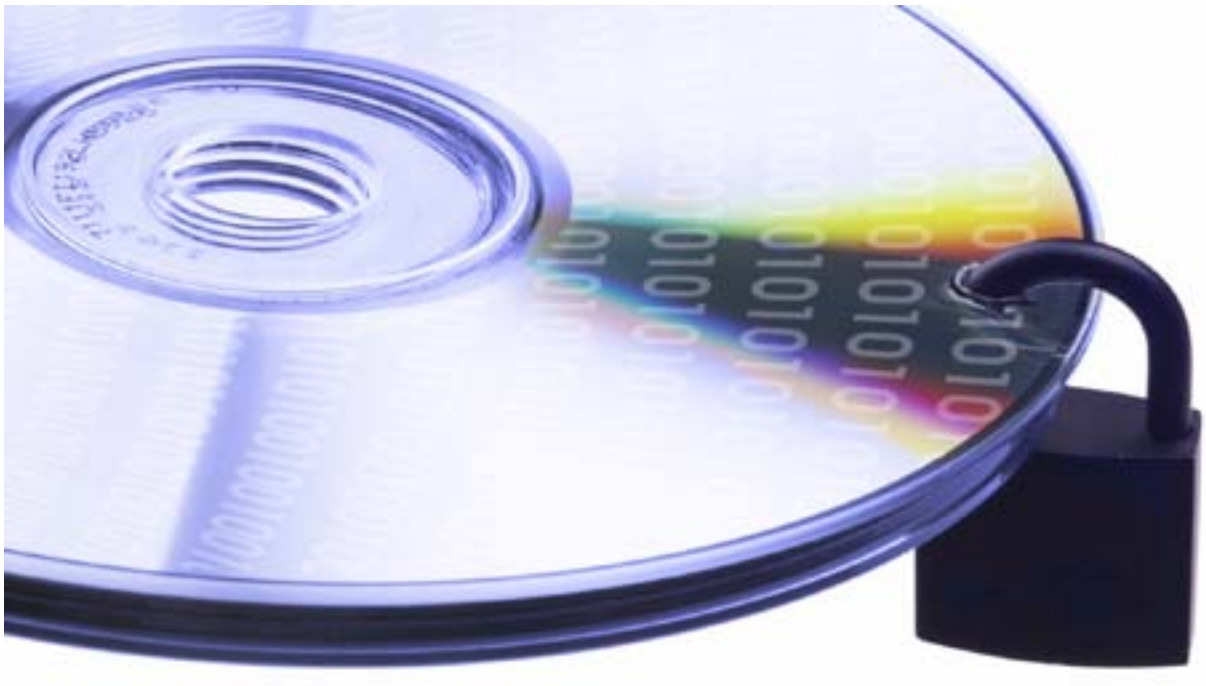
In his comments, the EDPS welcomed the safeguards included in the draft measures and the fact that there is an EU approach to security scanners, as this can guarantee legal certainty as well as a consistent level of protection of fundamental rights. However, he questioned the **necessity** and the **proportionality** of such measures and highlighted that **data protection legislation is applicable**.

The EDPS also **regretted that body scanners providing a detailed image of the body will be allowed**, especially given that preference could have been given to a less privacy-intrusive device (i.e. a body scanner showing a "stick figure" instead of the human body).

3.7. Cross-border enforcement

3.7.1. Intellectual Property Rights Enforcement Directive

On 8 April 2011, the EDPS responded to a public consultation launched by the European Commission on the application of the Intellectual Property Rights Enforcement Directive. The EDPS provided a broad overview of the data protection issues that



Enforcement of intellectual property rights on the Internet requires adequate data protection safeguards.

can arise in the context of enforcing intellectual property rights on the internet. The EDPS highlighted that the enforcement of intellectual property (IP) rights on the internet poses important challenges and requires adequate data protection safeguards. This is particularly applicable when carrying out monitoring of internet activity to find alleged infringers, or when collecting personal data information (such as a subscriber name linked to a concrete IP address) from intermediaries such as Internet Service Providers.

The EDPS stressed the importance of **striking a balance between the fundamental right to data protection and the right to intellectual property**. He accepted that the current provisions in the Directive - based on striking the balance in line with the commercial scale of the infringement - were appropriate, although clarification is still necessary in some areas.

Finally the EDPS made some recommendations to assist the Commission in taking a more prospective view. In particular, **data protection should be taken into account in the evaluation of the implementation of the current Directive**, its follow up and during possible future legislative modifications.

3.7.2. Customs enforcement of intellectual property rights

On 12 October 2011, the EDPS adopted an opinion on the proposal for a Regulation concerning customs enforcement of intellectual property rights. The EDPS welcomed the specific reference in the proposal to the applicability of Directive 95/46/EC and Regulation (EC) 45/2001 to the personal data processing activities covered by the Regulation.

The EDPS also highlighted the data subject's right to information, the need to devise a "data protection compliant" model application form, the specification of a time limit for the retention of personal data submitted by the right holder, both at national and at Commission level and the need for clarification of the legal basis for the establishment of a new central database of the Commission (COPIS).

3.7.3. Jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

On 20 September 2011, the EDPS commented on the proposal for a Regulation on jurisdiction and recognition and enforcement of judgments in civil and commercial matters. The EDPS highlighted the importance, equally in the area of data protection, of facilitating the settlement of cross-border disputes. The EDPS emphasised the need for further reflection on some of the issues raised in the proposal, also in the context of the ongoing review of the data protection framework in the EU:

- further reflection should be given to whether jurisdictional rules should protect the weaker party also in data protection litigation – as is already the case in employment, insurance and consumer protection matters;

- with regard to the retention of the exequatur for privacy, defamation and rights relating to personality and the possibility of denying recognition of judgments on public policy grounds in these cases, the EDPS stresses the need for a strict interpretation of those exceptions;

- it is not clear whether the above exception for privacy rights is intended to also cover violations of legal rules for the processing of personal data as provided for in the Data Protection Directive and if so, to what extent this may be the case. This may create problems of interpretation and will not contribute to the legal certainty that the proposal aims to establish;

- further reflection should be undertaken on how to better align the courts' jurisdiction with the competence of data protection authorities.

3.7.4. European Account Preservation Order

On 13 October 2011, the EDPS adopted an opinion on a proposal for a Regulation creating a European Account Preservation Order to facilitate cross-border debt recovery in civil and commercial matters. The EDPS was pleased to see the efforts taken to address the different data protection issues that arose from the proposed instrument of an EAPO. In particular, he appreciated the application of and the references to the principle of necessity.

Cross-border debt recovery involves processing of personal data.

However, the EDPS maintained that the proposed Regulation required further improvement and clarification. The EDPS recommended among other things:

- to consider including the possibility for the claimant to request the removal of his address details from the information provided to the defendant;
- to remove the optional data fields in Annex I to the Regulation (the telephone number and email address of the defendant) if the actual need is not proven;
- to restrict the information provided by the claimant to what is necessary in order to identify the defendant and to determine his or her bank account(s).

3.8. Public health and consumer affairs

3.8.1. Consumer Protection Cooperation System

On 4 May 2011, the EDPS issued a legislative opinion commenting on the legal framework for the Consumer Protection Cooperation System (CPCS). The CPCS is an IT system designed and operated by the Commission. The CPCS facilitates cooperation among competent authorities in the EU Member States and the Commission in the area of consumer protection. In the framework of their co-operation, competent authorities exchange information including personal data.

The EDPS welcomed the fact that the CPCS Regulation has been complemented over time with an implementing decision and a set of data protection guidelines which, combined, provide more details on the actual processing as well as specific data protection safeguards.

The main recommendations of the legislative opinion included the following:

- regarding the **retention period**, mutual assistance requests should be closed within specifically designated time-limits. Unless an investigation or enforcement is ongoing, alerts should be withdrawn and deleted within six months of issuance. Additionally, the Commission should clarify and reconsider the purpose and proportionality of keeping all data relating to closed cases for five additional years;
- the Commission should re-assess what additional technical and organisational measures could be taken to ensure that privacy and data protection are "designed" into the CPCS system architecture (**privacy by design**) and that adequate controls are in place to ensure data protection compliance and provide evidence thereof (**accountability**).

3.9. Other issues

3.9.1. OLAF Reform Regulation

On 1 June 2011, the EDPS adopted an opinion on a proposal for a Regulation which is intended to modify the current rules concerning investigations conducted by the European Anti-fraud Office (OLAF). The aim of the proposal is to increase the efficiency, effectiveness and accountability of OLAF, while safeguarding its investigative independence.

The EDPS supported the objectives of the proposed amendments and welcomed the proposal. Despite the overall positive impression, the EDPS considered that the proposal could be further improved in the protection of personal data without jeopardising the objectives that it pursues.

The EDPS, therefore, made a number of recommendations that should be addressed by modifying the text and in particular that the proposal should:

- clearly mention the **right to information** of the different categories of data subjects (suspects, witnesses etc.), as well as the **right of access and rectification** in relation to all phases of the investigations carried out by OLAF;

- clarify the relationship between the need for **confidentiality of the investigations** and the data protection regime applicable during the investigations;

- clarify the general data protection principles on the basis of which OLAF can **transmit and receive information**, including personal data, with other EU bodies and agencies and give the Director General the task of ensuring that a **strategic and comprehensive overview of the different processing operations** of OLAF is carried out, kept up to date and made transparent.

3.9.2. EU Financial Regulation

On 15 April 2011, the EDPS adopted an opinion on the Commission proposal revising the financial rules applicable to the annual budget of the European Union (EU Financial Regulation). The proposal covers several matters which involve the processing of personal data by EU institutions and entities at Member State level.

One of the most significant new elements introduced by the proposal is the potential publication of decisions on administrative and financial penalties. Such publication would entail the disclosure of information about the person concerned in an identifiable way. The EDPS believes that this provision as drafted does not meet the requirements of data protection law.

To better comply with data protection rules, it should be improved by explicitly indicating the purpose for the disclosure and by ensuring the consistent application of the possibility, of what is in fact naming and shaming of persons, together with the use of clear criteria to demonstrate the necessity of the disclosure.

The EDPS recommendations also covered the following:

- **whistleblowers**: the legislator should ensure the confidentiality of whistleblowers' identity during investigations, except in cases where it contravenes national rules regulating judicial procedures;

- **publication of information on the recipients of funds** deriving from the budget: the Regulation should explicitly indicate the purpose and explain the necessity for the disclosure of information on the recipients of funds deriving from the budget;

- **Central Exclusion Database**: the proposal provides for the setting-up of a database containing details of individual and company candidates excluded from participation in tenders. Access to the database by third country authorities should comply with the specific data protection rules related to third country transfers.

3.9.3. European statistics on safety from crime

On 19 September 2011, the EDPS adopted an opinion on the Commission proposal for a Regulation on European statistics on safety from crime. The proposal aimed to implement a new EU survey on safety from crime. The survey would include detailed questions on possible incidents of sexual and physical violence that the respondents might have suffered within or outside the couple, on past relationships, on their socio-demographic background and on their feelings of safety and attitudes to law enforcement and security precautions.

The EDPS stated that he is aware of the importance of the development, production and dissemination of statistical data. However, he is **concerned about questions related to physical and sexual offences** and about the **possibility of identifying alleged victims and aggressors**. He made a number of recommendations to reduce the risk of unnecessary direct or indirect identification, to ensure that the categories of personal data to be collected and processed are relevant and not excessive for the specific purpose and to implement adequate technical and organisational measures to ensure the confidentiality and security of personal data until they are made anonymous in line with data protection principles.

3.9.4. Transport

On 5 October 2011, the EDPS adopted an opinion on the Commission proposal to revise the EU legislation on tachographs – the device used in road transport to monitor driving times and rest periods of professional drivers – as a means of checking compliance with social legislation in the field. The revision is meant to make use of new technological developments to improve the effectiveness of digital tachographs against manual ones, notably through the use of geo-location equipment and remote communication facilities. The initiative invades the **privacy of professional drivers** in a very visible way, as it allows the constant monitoring of their whereabouts as well as remote surveillance by control

Introduction of a new digital tachograph could turn out to be very privacy-invasive.

authorities that will have direct access to the drivers' personal data stored in the system.

The EDPS emphasised that specific **data protection safeguards** are needed to guarantee a satisfactory level of data protection in the system, in particular:

- the installation and use of devices for the direct and principal purpose of allowing employers to **remotely monitor in real time the actions or whereabouts of their employees** should be excluded;
- the **general modalities of the processing of personal data** in tachographs should be set out clearly in the Proposal, such as the type of data recorded in tachographs and in geo-location equipments, the recipients and the time limits for data retention;
- the **security requirements** for the digital tachograph laid down in the Proposal need to be further developed, in particular to preserve the confidentiality of the data, to ensure data integrity and to prevent fraud and unlawful manipulation;
- the introduction of any technological update (e.g. remote communication, Intelligent Transport Systems) in tachographs should be duly supported by **privacy impact assessments** to assess the privacy risks raised by the use of these technologies.

These safeguards will also be relevant in the wider context of geo-location technologies: while these technologies can help to improve the efficiency and quality of transport, they also entail a risk of heightened surveillance of drivers.

3.9.5. Common Agricultural Policy after 2013

On 14 December 2011, the EDPS adopted an opinion on the legal proposals for the Common Agricultural Policy after 2013. The EDPS observed that many aspects central to data protection were not included in the proposals, but will be regulated by implementing or delegated acts. The EDPS recommended that at least the following elements be regulated in the proposals to ensure legal certainty:

- the **specific purpose** of every processing operation should be explicitly stated;
- the **categories of data** to be processed should be foreseen and specified because, in many cases, the scope of the processing was not clear;
- **access rights** should be clarified, in particular as regards access to data by the Commission - it should be specified that the Commission can only process personal data where necessary, for example, for control purposes;
- maximum **retention periods** should be laid down, as for some cases in the proposals, only minimum retention periods are mentioned;
- the **rights of data subjects** should be specified, especially as regards the right of information to beneficiaries and to third parties;
- **the scope and the purpose of transfers to third countries** should also be specified and the requirements laid down by the data protection legislation be respected.

Security measures should also be envisaged, especially with regard to computerised databases and systems. In addition, **data relating to offences or suspected offences** could be processed (for example, in relation to fraud), so the processing may be subject to prior checking by the EDPS or by national data protection authorities.

3.9.6. Fisheries policy control

This opinion, published on 28 October 2011, dealt with some technical aspects relating to a Commission Regulation implementing the fisheries control system. The EDPS had already issued an opinion in March 2009 on a related Regulation, but was nonetheless not consulted by the Commission before it adopted the current Regulation.

The activities of fishing vessels are subject to systematic and detailed monitoring through advanced technological means, including satellite tracking devices and computerised data-bases, tracing and retaining location data such as the geographical position, course and speed of fishing vessels. All these data are systematically cross-checked, analysed and verified through computerised algorithms and automated mechanisms in order to spot inconsistencies or suspected infringements.

As long as these data relate to identified or identifiable individuals (e.g. the master of the vessel, the

The activities of the fishing vessels are subject to systematic and detailed monitoring through advanced technological means.

owner of the vessel, or the members of the crew), such monitoring involves the **processing of personal data**. It is, therefore, important that the control system is well-balanced and that adequate safeguards are put in place in order to avoid the rights of the persons involved being unduly restricted.

3.10. Public access to documents containing personal data

The EDPS has addressed from the outset the sometimes complicated relationship between EU rules on **public access to documents** and EU rules on **data protection**. He first tackled the issue by providing guidance to EU institutions. In 2005, for example, the EDPS published a background paper entitled 'Public access to documents and data protection', which contained guidelines for EU institutions and bodies.

Part of the analysis presented in this background paper is no longer valid in light of the European Court of Justice judgment in the Bavarian Lager Case (see below 3.11.1). Therefore, on 24 March 2011, the EDPS published a background paper on public access to documents containing personal data, **to serve as guidance for EU institutions**. The paper explains the updated EDPS position on the matter following the ruling of the European Court of Justice in the *Bavarian Lager* case on the reconciliation of the fundamental rights to privacy and data protection with the fundamental right to public access to documents and transparency.

In case of public disclosure of personal data by the EU institutions, a proactive approach would ensure that the persons concerned are well-informed and able to invoke their data protection rights. It would also be beneficial to the institutions, as it would reduce future administrative burdens for those responsible for data processing and those who deal with public access requests.

The EDPS encourages the EU administration to develop **clear internal policies**, creating a presumption of openness for certain personal data in specified cases (e.g. documents containing personal data relating solely to the professional activities of the person concerned). The EDPS maintains that a change to the rules on public access is needed and he encourages the Council and Parliament to accelerate the pending revision process.

3.11. Court matters

3.11.1. EDPS participation in court proceedings

2011 was a busy year for the EDPS with regard to participation in proceedings before the European courts. The agents of the EDPS presented the EDPS' position in hearings before the courts in four cases, three of which have already led to a court ruling.

In *V. vs. European Parliament* (Case F-46/09), the EDPS was invited to intervene by the Civil Service Tribunal. The case concerned the allegedly illegal transfer of medical data between the medical services of the Commission and the European Parliament. The EDPS pleaded in favour of the applicant, arguing that the transfer was contrary to data protection rules, as it was not necessary and lacked a proper legal basis. In its judgment of 5 July 2011, the Civil Service Tribunal ruled in favour of the applicant, following the reasoning of the EDPS.

The three other cases all concerned the relationship between the EU rules on public access to documents and the EU rules on data protection. As outlined in 3.10, the EDPS was involved in this matter. The three cases can be seen as the legal follow-up to the leading *Bavarian Lager* ruling of the Court of Justice on 29 June 2010 (Case C-28/08 P). The EDPS explained his position in the three hearings, as set out in the additional background paper of 24 March 2011.

In its ruling of 7 July 2011, *Valero Jordana v. Commission* (Case T-161/04), the General Court considered that the Commission had been wrong in not assessing the request for public access to certain personal data under the data protection rules. This conclusion was in line with the EDPS' submissions to the Court argument.

In his interventions, the EDPS aims to clarify the perspective of data protection.

In the ruling of 23 November 2011, *Dennekamp v. European Parliament* (Case T-82/09), the General Court concluded that the applicant, a journalist asking for the names of Members of the European Parliament who were participating in an additional pension scheme, had not demonstrated the necessity of having the data made public. The EDPS had defended the opposite view, considering that a balance of the different interests involved should have led to disclosure of the data to the journalist.

The third case, *Egan & Hackett v. European Parliament* (Case T-190/10), has not, at the time of writing, led to a ruling of the General Court. This case concerned a request for access to the names of assistants of Members of the European Parliament.

In addition to these four cases, the EDPS has intervened in Commission v. Austria (Case C-614/10), an infringement case against Austria on the lack of independence of the Austrian data protection authority. The EDPS submitted a statement in intervention, supporting the Commission's conclusion that the way in which the Austrian data protection authority is embedded in the institutional structure of Austria does not sufficiently ensure its independence.

Finally, ENISA brought a case before the General Court against a decision of the EDPS on a complaint (Case T-345/11). The application was declared manifestly inadmissible on procedural grounds.

3.11.2. Data protection case law

The European courts issued several other rulings with data protection relevance. Three Court of Justice rulings are briefly outlined as follows.

In *Deutsche Telekom* (Case C-543/09) questions were raised on whether under the e-privacy Directive, an undertaking assigning telephone numbers to its subscribers was allowed to provide data relating to these subscribers to another undertaking whose activity consists of providing publicly available directory enquiry services without renewed consent of the persons involved. The Court considered in its ruling of 5 May 2011 that as the subscribers were already correctly informed of this possibility, renewed consent was not needed.

In its ruling in *ASNEF and FECEMD* of 24 November 2011 (Joined Cases C-648/10 and C-469/10), the Court of Justice replied to a Spanish court which had asked for clarification on a provision in the data protection Directive, which allows the processing of personal data if this serves a legitimate interest and is not outweighed by the interest of the data subject involved. In Spanish law this was only possible with regard to personal data that had already been made publicly available. According to the Court, this national restriction is not in line with the Directive which has direct effect on this point.

On 24 November 2011, the Court of Justice issued a preliminary ruling in a Belgian case, concerning an obligation on an Internet Service Provider (Scarlet Extended) to monitor the internet behaviour of its consumers in order to prevent breaches of intellectual property rights (Case C-70/10). The Court concluded that the obligation amounted to a general monitoring obligation which is forbidden under EU rules on e-commerce. The Court also noted that such an obligation would not constitute a fair balance between the enforcement of intellectual property rights and several fundamental rights and freedoms laid down in the Charter on Fundamental rights, amongst which is the right to data protection.

3.12. Future technological developments

In the so-called Information Society or Digital World, citizens, customers, administrations, and enterprises interact more than ever before thanks to technology. Technology is making the production, exchange and storage of information (including personal data) easier and is making traditional barriers such as geographical location, language or even infrastructure costs increasingly less relevant.

Furthermore, new technological developments are blurring the frontiers between the digital and real world (data exists in the digital arena but data subjects, data controllers and data processors do not); sooner rather than later both worlds will converge into a single reality with common rules. Technology is becoming increasingly accessible and easier to use and those who use it are not only data subjects but often also data controllers.

From 2012 onwards, the EDPS anticipates the following six topics assuming particular importance:

• **Increased Processing in the Cloud**. The 'cloud' paradigm has been around for some years. With sufficient scale, the cloud is now bringing noticeable benefits in terms of cost reduction and thus convincing enterprises, government organisations and citizens to move their data processing operations

into it. However it brings new challenges from a data protection point of view, such as, among others: (i) data controllers losing control over data processing operations due to the complexity of the scenarios arising, (ii) de-localisation of data and interplay of different jurisdictions in conjunction with the lack of harmonisation of data protection laws at international level, (iii) an increase in the number of players involved in data processing operations and a blurring of their responsibilities, (iv) massive data processing by individuals acting as data controllers without due knowledge of their obligations and (v) significant challenges for security and the enforcement of data subjects' rights.

Storage capacity, processing power and network bandwidth costs continue to drop in all the variants of cloud computing (as infrastructure, as a platform or as a service) to the point that the traditional link between volume of data and the cost of associated infrastructure will be soon broken i.e. as infrastructure costs are lowered, entry barriers to process large data operations disappear. This phenomenon will allow individuals and small enterprises to carry out massive data processing operations that, up to now, only governments and big corporations could afford.

• **Increased processing on smart mobile devices.** The possibilities that smart mobile devices offer are also growing at an accelerated pace. Today's devices are always on and able to share, modify and process information in real time. New generation devices will have more power, better interfaces, more connectivity, more storage capacity and will be seamlessly integrated with the cloud. In 2012, quad-core processors will become common in smart mobile devices, deployment of LTE networks([13]) will take place, devices will connect to the cloud to process our voice commands, augmented reality will continue to grow and biometric interfaces such as face or voice recognition will become standard.

In addition to the enhanced capabilities of the new devices users will have all the computing power of the cloud, packaged in an easy-to-use integrated kit. Individuals will be able to generate information and upload it into the cloud on an unprecedented scale. They will continuously process their own personal data and the personal data of others.

• **IPv6.** In 2011, the last remaining IPv4 addresses (the current network addressing schema used in the Internet) were assigned and focus turns now to IPv6. This new standard allows, among other things, a virtually unlimited IP address space and consequently, the allocation of unique identifiers to every single device connected to the network (for instance RFID devices using IP). IP addresses will no longer be a scarce resource and it will be cheaper to assign a unique identifier than a dynamic address.

In this context, the Resolution adopted at the International Privacy Conference in Mexico([14]) on IPv6 is relevant; this resolution requires unique identifiers not to be used without the consent of end users and to allow end users to use temporary and volatile IPv6 addresses (dynamic addresses) by default. Security issues that might arise in the transition from IPv4 to IPv6, should also be taken into consideration.

• **New Human to Machine Interfaces** will become available. Current tablets and smart phones have made communication between humans and machines easier. Soon these interfaces will be incorporated in other devices such as security systems, cars, televisions and gaming systems. Touchable, wearable, visual and voice interfaces will become part of everyday life. Information systems designed to assist humans will be able to sense and interpret faces, movements, voices, behaviour and even health. Indeed, intelligent systems will soon be able to monitor how humans feel physically and even psychologically based on behavioural patterns. An application for e-health services that remotely monitors patients so they can stay at home instead of in a hospital benefits the individual and can potentially bring cost savings but should not be implemented at the expense of the right to data protection and privacy.

These developments will have enormous influence from a societal point of view and data protection in particular, will have to play an increasing role to ensure that appropriate safeguards are foreseen and that the principle of privacy-by-design is applied in the implementation of these technologies. Solutions can be found to obtain full functionality while preserving the privacy of individuals if systems are well designed from inception.

([13]) LTE is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using new modulation techniques The standard is developed by the 3GPP (3rd Generation Partnership Project). It provides for speeds that go up to 300 Mbit/s.

([14]) See also chapter 4.6 of this annual report.

• **Smart Grids.** Various upcoming grid technologies are starting to take shape, such as Vehicle to Grid (V2G), Outage Management Systems (OMS) or micro grids. In particular, utility companies (water and electricity mainly) have already started the deployment of advanced metering systems that will provide much more detailed information of consumption patterns to the utility provider and eventually also to the customer. This information will be used for better forecasting and adaptability of the network to consumer demand and hopefully will increase the efficiency in the use of scarce resources such as water or energy, especially by the automation of distribution networks.

However, the concept of smart grids is broad and can have a far-reaching impact as smart devices connect to the grid and exchange information. Notwithstanding the possible economic benefits, it is also clear that an unprecedent amount of information about individuals' behaviour will be transmitted and processed by a myriad of actors.

Consequently, in order to preserve the right to data protection of individuals, these data processing operations have to be balanced and data protection principles such as proportionality, necessity or legitimacy need to be correctly applied.

• **Increased Security Issues** will make cyber security more important than ever. Whilst the value of the cyber criminal economy as a whole is not yet known, the most recent estimate of global corporate losses alone stands at around EUR 750 billion per year.([15]) The number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and international. There are clear indications of a growth in organised crime groups, new groups born from hackers and internet culture and even the involvement of some governments.

Special attention should be paid to the various legal rules, in order to ensure that appropriate security measures are taken in order to protect personal data, in the harmonisation of these measures and the procedures to notify data breaches to the relevant authorities and the affected data subjects. In particular, it should be noted that the new general Data Protection Regulation proposed by the Commission will extend the obligation to notify data breaches to all data controllers([16]).

([15]) http://ec.europa.eu/home-affairs/policies/crime/crime_cybercrime_en.htm

([16]) Directive 2002/58 as amended by 2009/136 only establishes the obligation to notify personal data breaches for electronic communications service providers.

Information systems are becoming critical elements in our daily lives and individuals have to rely on technology and systems that they do not fully understand. Consequently, they need third parties to provide them with assurance mechanisms that can warrant the privacy and security of such information systems. In this context, a steady growth is foreseeable in the certification business and also in the processes providing accountability of good practices.

3.13. Priorities for 2012

In January 2012, the EDPS will publish his sixth public inventory as an advisor on proposals for EU legislation, setting his priorities in the field of consultation for the year ahead. The EDPS faces the challenge of fulfilling his increasing role in the legislative procedure, by delivering high-quality and well-appreciated advice with increasingly limited resources.

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

- There is an increasing tendency to endow administrative authorities, both at the EU and national levels with powerful information gathering and investigative tools. This is particularly the case in the area of freedom, security and justice and in relation to the revision of the legislative framework concerning financial supervision;

- EU legislation increasingly facilitates significant exchanges of information between national authorities, frequently involving EU bodies and large-scale databases (with or without a central part) of increasing size and processing power. This requires careful consideration by policy makers and actors when setting out data protection requirements during the legislative procedure, because of the serious consequences these exchanges can have for the privacy of citizens, e.g. by facilitating the monitoring of citizens' lives;

- Recent years have been characterised by significant technological developments, mainly due to the widespread use of internet and geolocation technologies. Such developments

have a significant impact on a citizen's right to privacy and data protection.

Such policy and technological developments underline that data protection and privacy have become truly horizontal issues. This also means that there will be more demand for EDPS advice on proposed legislative measures.

In light of this, the EDPS has identified issues of strategic importance that will form the cornerstones of his consultation work for 2012, while not neglecting the importance of other legislative procedures where data protection is concerned.

The EDPS is therefore committed to devoting substantial resources in 2012 to the analysis of proposals of strategic importance. In addition, the EDPS has identified a number of initiatives of less strategic importance which may nonetheless have data protection relevance. The fact that the latter are included in the EDPS Inventory implies that they will be regularly monitored, but does not mean that the EDPS will always issue an opinion or formal comments on such initiatives.

The main EDPS priorities, as identified in his inventory, are as follows:

a. Towards a new legal framework for data protection
   - Revision of EU data protection framework

b. Technological developments and the Digital Agenda, IP rights and Internet
   - Pan European framework for electronic identification, authentication and signature
   - Internet monitoring (e.g. enforcement of IP rights, takedown procedures)
   - Cloud computing services
   - eHealth

c. Further developing the Area of Freedom, Security and Justice
   - EU-PNR
   - EU-TFTS
   - Border controls
   - Review of Data Retention Directive
   - Negotiations on agreements with third countries on data protection

d. Financial sector reform
   - Regulation and supervision of financial markets and actors

4 COOPERATION

4.1. Article 29 Working Party

The Article 29 Working Party is the independent advisory body set up under Article 29 of the Data Protection 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.([17])

Its tasks are laid down in Article 30 of the Directive and can be summarised, as follows:

- provide expert opinion from Member State level to the European Commission on matters relating to data protection;
- promote the uniform application of the general principles of the directive in all Member States through cooperation between data protection supervisory authorities;
- advise the Commission on any measures affecting the rights and freedoms of natural persons with regard to the processing of personal data;
- make recommendations to the public at large and in particular to EU institutions, on matters relating to the protection of persons with regard to the processing of personal data in the EU.

The EDPS has been a member of the Article 29 Working Party (WP29) since early 2004 and considers it to be a very important platform for cooperation with national supervisory authorities. It is also evident that the Working Party should play a central role in the consistent application of the directive and in the interpretation of its general principles.

In 2011, as in 2010, the Working Party focused its activities on the four main strategic themes identified in its 2010-2011 work programme, notably:

- implementing the revised e-Privacy Directive and preparing a future comprehensive legal framework;
- addressing globalisation;
- responding to technological challenges;
- making the Working Party and data protection authorities more effective.

To this end, the Working Party adopted several documents, among which are:

- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications (WP 180);

([17]) The Working Party is composed of representatives of the national supervisory authorities in each Member State, a representative of the authority set up for the EU institutions and bodies (i.e. the EDPS), and a representative of the Commission. The Commission also provides the secretariat of the Working Party. The national supervisory authorities of Iceland, Norway and Liechtenstein (as EEA partners) are represented as observers.

- Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of **passenger name record** data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (WP 181);

- Opinion 15/2011 on the definition of **consent** (WP 187);

- Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (WP 188).

The Working Party also took positions in the form of letters on several issues, among which were the implementation of the Terrorist Financing Tracking Programme (TFTP) and the self-regulatory framework on Online Behavioural Advertising (OBA) developed by the industry.

The EDPS actively contributed to the work of the WP29 in different areas. He was particularly involved in the work of several subgroups, including the technology subgroup, the BTLE subgroup (Border Travel and Law Enforcement) and the key provisions subgroup, the aims of which are to provide for a common interpretation of essential provisions of Directive 95/46/EC. In the context of this last subgroup, he was rapporteur for the opinion on the notion of **consent** (Opinion 15/2011). The EDPS was also deeply involved in the work of the subgroup on the 'future of privacy' in relation to the initiative of the Commission for a new data protection framework.

The EDPS also cooperates with the national supervisory authorities to the extent necessary for the performance of his duties, in particular by exchanging all useful information and requesting or delivering assistance in the performance of their tasks (Article 46(f)(i) of the Regulation). This cooperation takes place on a case by case basis.

Direct cooperation with national authorities is an element of growing importance in the context of the development of large-scale international systems such as Eurodac, which require a coordinated approach to supervision (see Sections 4.2 and 4.3).

4.2. Coordinated supervision of Eurodac

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

Technological challenges were one of the main strategic themes of the Articles 29 Working Party in 2011.

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.([18])

In 2011, the Eurodac Supervision Coordination Group, composed of representatives of the national data protection authorities and the EDPS, based its activities on the 2010-2011 work programme, adopted in early 2010.

The Group held two meetings in Brussels, one in June and one in October 2011. The October meeting represented the first meeting entirely organised by the EDPS and was considered by participants as a success in terms of organisation and outcome.

4.2.1. Advance Deletion Report

One of the Group's most significant achievements of the year was the coordinated inspection on advance deletion. Advance deletion refers to the deletion of data in the central unit before the end of the retention period. This can occur if a person leaves the EU or acquires citizenship or a resident's permit, for example. Deleting such persons from the database safeguards their rights and increases data quality. One of the aims of this exercise was to provide a state of play on the application of advance deletion rules in the Member States and to explore whether there is a need for alternative solutions.

The final report confirms that many Member States have already implemented appropriate procedures; those that have not yet done so usually experience very few or no cases in which advance deletion would have been necessary. Recommendations included establishing such procedures where they are still missing, providing better information to concerned persons and working towards better statistics on the phenomenon.

The report has been sent to the main EU institutional stakeholders, as well as to relevant international organisations.

4.2.2. New exercise in 2012: unreadable fingerprints

As the reform of the Eurodac Regulation did not move forward in 2011, the Group had to adapt its work programme accordingly, postponing several items. This adaptation introduced a new coordinated inspection on the issue of unreadable fingerprints, to be carried out in 2012.

The processing of biometric data such as fingerprints poses specific challenges and creates risks which have to be addressed. In this context, the problem of so-called 'failure to enrol' - the situation in which a person finds that their fingerprints are not usable for some reason - is one of the main risks.

The main purpose of the exercise is to examine the current procedures applied in all Member States when this situation occurs and whether there is a need for new solutions. Similar to the advance deletion exercise, this investigation should be seen more as an exploratory exercise, which could then lead to:

- the identification of good practices (whether they take the form of technical features, internal guidelines or administrative practices) and an encouragement to use them widely;
- any further recommendations if the exercise shows that there are deficiencies in the current system.

4.2.3. Coordinated security audit questionnaire

During both meetings of Eurodac in 2011, the ongoing preparations for the coordinated security audit were discussed. On the basis of the methodology used in a national audit, efforts are being made to develop a common framework for security audit methodology, which can provide support to national authorities and at the same time ensure consistent and useful outcomes for Eurodac generally. Work will continue on this in 2012 with the aim of adopting a common framework by the end of the year.

4.2.4. Visa Information System

The launching of the Visa Information System (VIS) in October 2011 gave rise to an informal discussion within the Group on its supervision. The Group agreed on a gradual and pragmatic approach to be concluded by the end of 2012. This means that the next Eurodac meetings will dedicate a substantial portion of the agenda, albeit informally, to VIS.

([18]) Iceland, Norway, Switzerland and, since the entry into force of a protocol to this effect on 1 April 2011, Liechtenstein.

4.3. Supervision of the Customs Information System (CIS)

The aim of the Customs Information System (CIS) is to create an **alert system** within the **fight against fraud** framework so as to enable any Member State entering data in the system to request another Member State to carry out sighting and reporting, discreet surveillance, a specific check 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 in order to assist in preventing, investigating and prosecuting actions which are in breach of customs and agricultural legislation (the former EU 'first pillar') or serious contraventions of national laws (the former EU 'third pillar'). The latter part is supervised by a Joint Supervisory Authority 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[19] - i.e. EDPS and national data protection authorities - cooperate in line with their responsibilities in order to ensure coordinated supervision of CIS.

The Coordination Group shall:

(a) examine implementation problems in connection with the CIS operations;

(b) examine difficulties experienced during checks by the supervisory authorities;

(c) examine difficulties of interpretation or application of the CIS Regulation;

(d) draw up recommendations for common solutions to existing problems;

(e) endeavour to enhance cooperation between the supervisory authorities.

[19] 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.

In 2011, the EDPS convened two meetings of the CIS Supervision Coordination Group (in June and December). The meetings gathered the representatives of national data protection authorities, as well as representatives of the Customs Joint Supervisory Authority and Data Protection Secretariat.

In the June meeting, the Group elected Mr. Giovanni Buttarelli, Assistant EDPS, as Chair and Mr. Gregor König, Austrian representative and Chair of the Customs Joint Supervisory Authority, as Vice-Chair. The Group also discussed and adopted a work programme outlining its activities for 2011 and 2012 and confirmed its intention to fully cooperate with the Customs Joint Supervisory Authority in areas of common interest. In the December meeting, the Group discussed documents guiding its first inspections on access to the system and data subject rights, which will be carried out in 2012.

4.4. Police and judicial cooperation: cooperation with JSB/JSAs and WPPJ

The EDPS also cooperates with the authorities charged with the supervision of specific bodies or EU large-scale IT systems, such as the Joint Supervisory Bodies (JSBs) of Europol and Eurojust and the Joint Supervisory Authorities (JSAs) for the Schengen Information System (SIS) and the 'ex-third pillar' aspects of the Customs Information System (CIS). This cooperation takes the form of mutual information on items of common interest, such as those where the EDPS and the JSB/JSAs each supervise different parts of the same system.

In 2011, the cooperation related mainly to the CIS. Since the EDPS and the JSA of the CIS share a supervisory role for the same system, it is logical to coordinate their action as much as possible. Thus, the EDPS invited representatives of the JSA to attend meetings organised on the coordinated supervision of the CIS (see Section 4.3). In the same spirit, EDPS representatives were invited to parts of JSA meetings where items of common interest were discussed.

The EDPS also participates in the meetings and activities of the Working Party on Police and Justice (WPPJ). The WPPJ worked on several issues in 2011, such as the use of DNA profiles by law enforcement authorities (including exchange of DNA data via Interpol Gateway), establishment of a common supervisory policy and risk assessments with respect to processing of personal data in the area of law enforcement in Europe.

In 2011, the WPPJ also broached the subject of its own future in light of the growing involvement of the WP29 in areas traditionally dealt with by the WPPJ. At the European Conference (see point 4.5. European Conference below), the WPPJ was mandated to work towards the integration of its EU-related competences and expertise into the Article 29 Working Party, which in turn was invited to clarify the status of its subgroup on law enforcement and the possibilities for non-EU Member States to participate in its work.

4.5. European Conference

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

In 2011, the European Conference of Data Protection Commissioners took place in Brussels on 5 April 2011. The format for the meeting was exceptional: the conference was hosted by the EDPS, in close cooperation with the Article 29 Working Party which also met on the morning of the same day.

The conference included sessions dedicated to a variety of issues, including:

- overview of legal developments: Lisbon Treaty, EU legal framework, Convention 108, OECD guidelines...;
- role of the Article 29 Working Party;
- supervision in the Area of Freedom, Security and Justice.

Use of DNA profiles by law enforcement authorities was on the agenda of WPPJ.

The future framework for data protection was at that time still in preparation by the European Commission. It was a central theme of the discussions and led to the adoption of a Resolution on the need for a comprehensive data protection framework.

4.6. 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 33rd Annual Conference of Data Protection and Privacy Commissioners took place in Mexico City on 1-3 November 2011 and was entitled 'Privacy: The Global Age'. Its aim was to explore ways for building the relationships and tools necessary to protect the data of individuals beyond national borders.

There was also a pre-conference on 31 October in Mexico City entitled 'Privacy as Freedom', followed by two events on 1 November hosted by the Organisation for Economic Cooperation and Development and the Information and Privacy Commissioner of Ontario, Canada. The conference was an opportunity for data protection stakeholders in Europe to meet their peers from Canada, the United States, Latin America, Australia, New Zealand, China, Japan to name but a few.

The closing session witnessed the official presentation of the so-called Mexico Declaration, prepared by the hosting authority with contributions from other delegations. This declaration urges selected stakeholders to effectively cooperate in order to confront new challenges, one being how to effectively enforce data protection in a world of 'big data'.

One of the main achievements of the conference was the initiative taken to step up the global cooperation of Data Protection and Privacy Commissioners. An executive committee was installed - chaired by the Chairman of the Article 29 Working Party and participants from all over the world - to give more permanence to the International Conference between its annual meetings. Special emphasis will be given to global cooperation in privacy enforcement and a separate meeting on enforcement issues was announced for May 2012, in Montreal.

The list of distinguished speakers included Peter Hustinx, EDPS and Giovanni Buttarelli, Assistant Supervisor, who both moderated sessions at the conference.

The 34th International Conference will take place in Uruguay, in October 2012.

5 INFORMATION AND COMMUNICATION

5.1. Introduction

Information and communication play a key role in ensuring the **visibility** of the EDPS' main activities and in **raising awareness** both of the EDPS' work and of data protection in general. This is all the more important as awareness of the EDPS role and mission at EU level needs to be raised further, although significant progress has already been made. Indicators such as the number of information requests received from citizens, media enquiries and interview requests, the number of subscribers to the newsletter, as well as invitations to speak at conferences and website traffic all support the view that the EDPS is a point of reference for data protection issues at EU level.

The increased visibility of the EDPS at institutional level is pertinent for his three main roles i.e. the supervisory role in relation to all EU institutions and bodies involved in the processing of personal data; 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 data; and the cooperative role in relation to national supervisory authorities and the various supervisory bodies in the field of security and justice.

5.2. Communication 'features'

EDPS communication policy is shaped according to specific features that are relevant in view of the age, size and remit of the institution and the needs of its stakeholders. It tailors the tools available to the audiences concerned and is adaptable to a number of constraints and requirements.

5.2.1. Key audiences and target groups

The communication policies and activities of the majority of other EU institutions and bodies operate on a general level to address EU citizens as a whole. The EDPS' direct sphere of action is more distinct. It is primarily focused at EDPS stakeholders - the EU institutions and bodies, data subjects in general and EU staff in particular, EU political stakeholders and 'data protection colleagues'. As a result, EDPS communication policy does not need to engage in a 'mass communication' strategy. Instead, awareness of data protection issues among EU citizens in the Members States depends essentially on a more indirect approach, for instance via data protection authorities at national level.

This being said, the EDPS does communicate with the general public, via a number of communication tools (website, newsletter, awareness-raising events), regularly liaising with interested parties (study visits to the EDPS office, for instance) and participating in public events, meetings and conferences.

5.2.2. Language policy

EDPS communication policy takes into account the specific nature of its field of activity. Data protection issues may be viewed as fairly technical and

obscure for non-experts and the language in which the EDPS communicates is, therefore, adapted accordingly. When it comes to information and communication tools aimed at a diverse audience, clear and accessible language which avoids unnecessary jargon needs to be used. Continued efforts are therefore made in this direction, in particular when communicating with the general public and the general press, with the aim of correcting the excessive 'legal' image of data protection.

When considering more informed audiences (e.g. data protection specialists, EU stakeholders), a more specialised language is appropriate. Different communication styles and language patterns need to be used to communicate the same news.

Since 2010, the EDPS has been relaying his messages in his press and communication activities in at least three languages - English, French and German. The overall aim is to reach out to the widest possible audience.

5.3. Media relations

The EDPS aims to be as accessible as possible to journalists in order to allow the public to follow his activities. He regularly informs the media through press releases, interviews and background discussions. The handling of media enquiries allows for additional regular contacts with the media.

5.3.1. Press releases

In 2011, the press service issued 12 press releases. Most of these related to the EDPS work in the field of consultation and, more specifically, on **new legislative opinions** of direct relevance to the general public. Among the issues covered were the EU Data Protection Reform Strategy, the guidance for good practice on data protection and transparency, the EU system on Passenger Name Record, the EU financial regulation, the evaluation of the Data Retention Directive, online behavioural advertising, recording equipment in road transport, the neutrality of the Internet and the Internal Market Information System.

Press releases are published on the EDPS website and in the European Commission inter-institutional database of press releases (RAPID) in English, French and German. Press releases are distributed to a regularly updated network of journalists and interested parties. The information provided in press releases usually results in significant media coverage by both the general and specialised press. Press releases are also frequently published on institutional and non-institutional websites ranging from, among others, EU institutions and bodies, to civil liberty groups, academic institutions and information technology companies.

5.3.2. Press interviews

In 2011, the EDPS gave 14 direct interviews to journalists from print, broadcast and electronic media throughout Europe, with a significant number of requests coming from German, Austrian, Dutch, French and the EU specialised press.

This resulted in a number of articles in the international, national and EU press, whether general or specialised in information technology issues, as well as interviews on radios.

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 2011, including EU-US data transfers, the review of the EU legal framework for data protection and privacy concerns with regard to social networking, consumer profiling, rights of digital citizens, data retention and security.

5.3.3. Press conference

The EDPS held a press conference on 15 June 2011 at the European Parliament in Brussels to present the EDPS 2010 Annual Report and outline the main features of the EDPS activities in 2010 with regard to his supervisory, consultative and cooperative tasks (see section 5.7.1.).

The press conference provided Peter Hustinx, EDPS, and Giovanni Buttarelli, Assistant Supervisor, the opportunity to address the current dynamic context of EU data protection and future challenges as well as to answer questions posed by journalists.

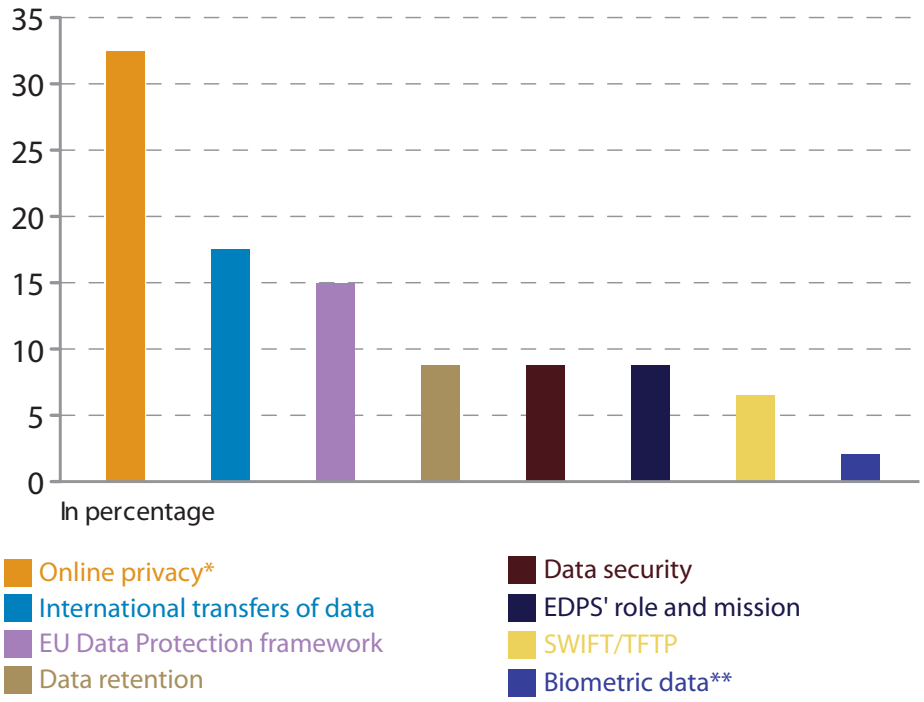
5.3.4. Media enquiries

In 2011, the EDPS received some 46 written media enquiries that included requests for EDPS comments and requests for clarification, position or information. Media attention in 2011 focused mainly on the issue of online privacy, in particular new online applications, such as geo-location applications, search engines and – the top-ranking area of enquiry - social networks.

Other issues of interest to the media included international transfers of data, the review of the EU legal framework for data protection, the Data Retention Directive, data security and provisions on data breaches, as well as the use and transfer of Passenger Name Records to the United States.

Peter Hustinx and Giovanni Buttarelli presenting EDPS Annual Report 2010 during a press conference.

Main topics for requests from the press in 2011



(*) Including new online applications, search engines and social networks.
(**) Including Schengen Information System.

5.4. Requests for information and advice

There was an increase of 39% in the number of enquiries for information or assistance received from citizens between 2010 and 2011 (196 requests compared to 141 in 2010). This evolution is the result of the more prominent profile of the EDPS within the data protection sphere, reinforced through the use of various information and communication tools.

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 (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.

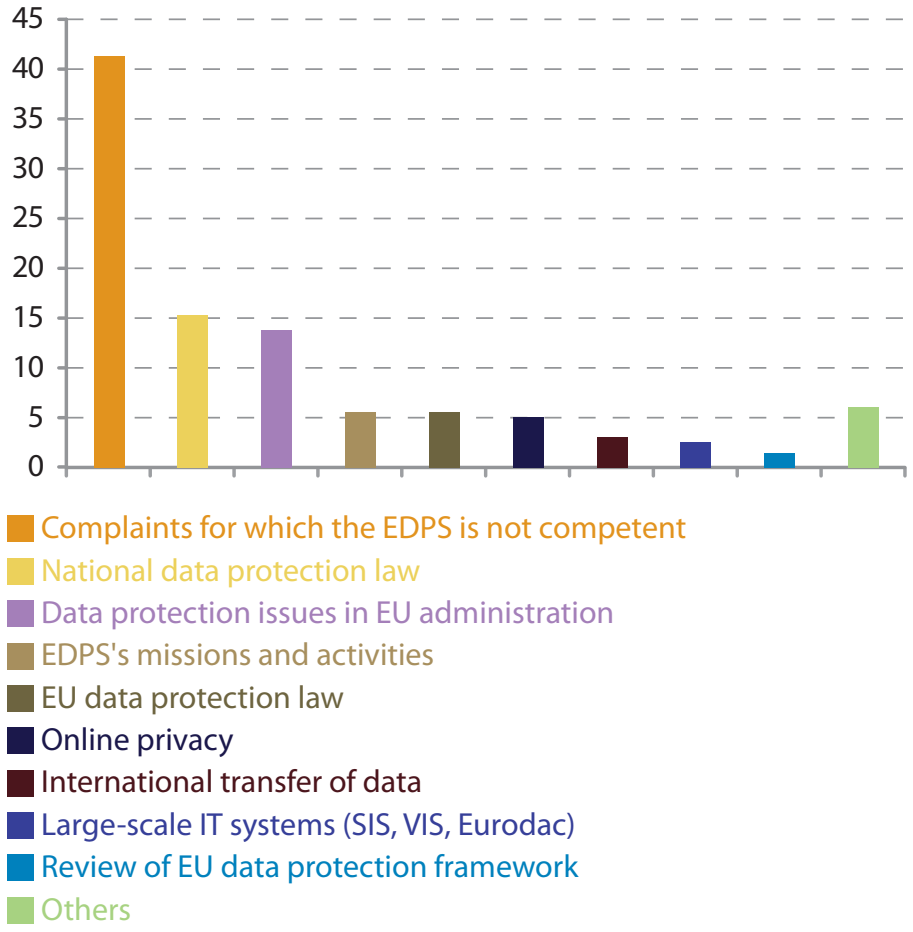
The largest category of requests received in 2011 concerned complaints from EU citizens about matters over which the EDPS has no competence. These complaints related mostly to alleged data protection breaches by public authorities, national or private companies and online services and technologies, such as online gaming, blogs, geo-location services, social networking and messaging tools. Other issues included the security of bank data, the right of access to documents held by national administrations, the dissemination of personal data to third parties without the consent of the person concerned and requests for appeal against a ruling from a national data protection authority. When complaints such as these fall outside the competence of the EDPS, a reply is sent to the complainant specifying 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.

The next sizeable category of requests received in 2011, related to data protection legislation in EU Member States and/or its implementation at national level. In such cases, the EDPS advises the individual to contact the relevant data protection authority and where appropriate, the European Commission Data Protection Unit.

The third main category of requests for information related to data protection issues within the EU administration, such as processing activities by EU institutions, bodies and agencies.

The remaining categories of information requests included enquiries about EDPS activities, role and missions, EU data protection legislation, online privacy, international transfer of data, large-scale IT systems such as VIS, SIS and Eurodac, and the review of the EU framework for data protection.

Main areas of information requests from the public in 2011



5.5. Study visits

As part of the efforts to further increase awareness of data protection and to interact with the academic world, the EDPS regularly welcomes visits from groups specialised in the field of European law, data protection and/or IT security issues. In 2011, the EDPS office welcomed four student groups from different countries. In December 2011, for instance, the EDPS office welcomed a group of German and European law students from the University of Cologne in Germany, presented its role and activities, and discussed data protection issues at EU level. Other groups of visitors included the Science and Technology Law Institute of Taipei (Taiwan), the Nanyang Technological University (Singapore) and the University Pierre Mendès France of Grenoble (France).

With a view to reaching out to a broader audience, the EDPS office also welcomed four groups or associations interested in data protection issues and privacy concerns: members of the German Evangelical Church, the association of the Young Europeans of Bordeaux (France), the Politieacademie (the Netherlands) and the Communication Sub-Committee of the Trainees of the European Commission.

5.6. Online information tools

5.6.1. Website

The website remains the EDPS' most important communication channel and information tool. It is updated on a daily basis. It is also the medium through which visitors have access to various documents produced as a result of EDPS activities (e.g. opinions on prior checks and on proposals for EU legislation, work priorities, publications, speeches of the Supervisor and Assistant Supervisor, press releases, newsletters, event information and so on).

Web developments

The most prominent development of the website in 2011 was an electronic platform for lodging complaints. The online complaint form facilitates the process of submitting complaints and speeds-up their processing by the EDPS services.

As announced in the Annual Report 2010, a 'press kit' section was also introduced on the website in order to provide media professionals with relevant materials and resources that can be used in their news articles and reporting interviews.

Between September and November 2011, an online survey was carried out on the quality of the EDPS website. The overall views of the website were positive: the majority of people found the website satisfactory in terms of the content. They also claimed that the information was accurate, up-to-date and easy to understand. Although the site was rated as quite easy to use, further improvements will be made in 2012 to the 'advanced search' function and the register.

In addition, an overhaul of the supervision and consultation sections is foreseen in order to enhance search options and navigation through thematic categories. Other improvements will include creating a Data Protection Officers' Corner and implementing the RSS feed feature.

Traffic and navigation

An analysis of the traffic and navigation data shows that in 2011, the website received a total of 65 599 unique visitors, including more than 6 000 per month in January, May and June.

After the homepage, the most regularly viewed pages were the 'Press and News', 'Supervision' and 'Consultation' pages, although the 'Publications' and 'Events' pages were also popular. The statistics also show that most visitors access the website via a direct address, a bookmark, a link in an email or a link from another site – such as the Europa portal or a national data protection authority's website. Search engines links are used only by a few visitors.

5.6.2. Newsletter

The EDPS newsletter remains a valuable tool for providing information on the EDPS' most recent activities and to draw attention to recent additions to the website. The newsletter provides information on the EDPS' most recent opinions on EU legislative proposals and on prior checks in his supervisory role. It also includes details of conferences and other events organised in the field, as well as recent speeches by the Supervisor and Assistant Supervisor. The newsletters are available in English, French and German on the EDPS website and a subscription feature is offered on the relevant page.

Four issues of the EDPS newsletter were published in 2011, with an average frequency of one issue every three months. The number of subscribers rose from 1 500 at the end of 2010 to approximately 1 750 by the end of 2011. Subscribers include members of the European Parliament, staff members from the EU institutions, staff of national data protection authorities, journalists, the academic community, telecommunication companies and law firms.

5.7. Publications

5.7.1. Annual Report

The annual report is a key EDPS publication. It provides an overview of EDPS activities in the main operational fields of supervision, consultation and cooperation during the reporting year and sets out the main priorities for the following year. It also describes what has been achieved in terms of external communication as well as developments in administration, budget and staff. A specific chapter is also dedicated to the activities of the EDPS' Data Protection Officer.

The report may be of particular interest to various groups and individuals at international, European and national 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

EDPS Annual Report 2010.

anyone seeking information on the protection of personal data at EU level.

The Supervisor and Assistant Supervisor presented the EDPS 2010 Annual Report to the European Parliament Committee on Civil Liberties, Justice and Home Affairs on 15 June 2011. The main features of the report were also presented at the press conference on the same day.

5.7.2. Thematic publications

Preparatory work has started on thematic fact sheets relating to data protection issues of strategic importance for the EDPS. The aim is to publish targeted information as guidance for the general public and other interested parties. The first set of fact sheets will cover issues such as data breaches, e-Privacy, the SWIFT/TFTP agreement and Passenger Name Record (PNR).

5.8. Awareness-raising events

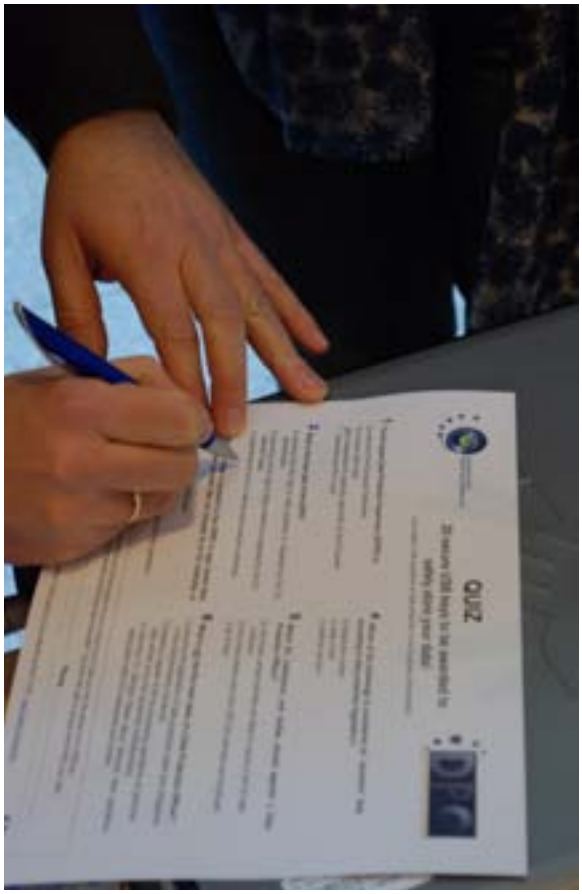
The EDPS is keen to seize relevant opportunities to highlight the increasing relevance of privacy and data protection and to raise awareness of the rights of data subjects as well as the obligations of the European administration in relation to these.

5.8.1. Data Protection Day 2011

The Member States of the Council of Europe and the European institutions and bodies celebrated the fifth European Data Protection Day on 28 January 2011. 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 EDPS uses this opportunity to stress the importance of privacy and data protection and in particular to raise awareness among EU staff of their rights and obligations in the field. For each Data Protection Day, an information stand is set up and operated by members of the EDPS office and its data protection officer on the premises of the Council, the European Commission and the European Parliament in cooperation with the data protection officer of the respective institution. Visitors have the opportunity to ask questions and to test their knowledge of EU data protection in a quiz.

In 2011, the EDPS renewed this specific activity, while investing further efforts in raising awareness among EU staff. A video message from the Supervisor and Assistant Supervisor was also circulated to institutional stakeholders and made available on the EDPS website, in both a long and short version, to present the role of the EDPS and outline the challenges for the year.



Visitor filling in a quiz during Data Protection Day 2011 on the EDPS information stand.

The EDPS also participated in various events organised on the occasion of Data Protection Day, such as the international conference on 'Computers, Privacy and Data Protection', that serves as a bridge for policymakers, academics, practitioners and activists to discuss emerging issues of privacy, data protection and information technology. For this fourth international event, the conference theme was 'European Data Protection: In Good Health?'. It took place on 25-27 January 2011 and included two one-day events on 'eHealth' and surveillance and a round table on body scanners. Members of the EDPS secretariat took part in panel discussions and Peter Hustinx gave the concluding notes at the conference.

5.8.2. EU Open Day 2011

On 7 May 2011, the EDPS participated as usual in the Open Day at the European institutions, organised at the European Parliament in Brussels. The EU Open Day offers an excellent opportunity for the EDPS to increase general public awareness of the need to protect privacy and personal information.

Staff members from the EDPS secretariat were present to answer questions from visitors at the EDPS stand in the main building of the European Parliament. As with the EDPS stand for Data Protection Day, there was a quiz on privacy and data protection at EU level and information materials were also distributed to visitors. The installation of a thermic camera linked to a large screen was a major attraction at the stand. Although there was no direct link with the processing of personal data, citizens were made aware, in a striking and fun way, of the potential privacy risk posed by new technology.

Visitors playing with a thermic camera on the EDPS stand during EU Open Day 2011 at the European Parliament.

6 ADMINISTRATION, BUDGET AND STAFF

6.1. Introduction

The entry into force of the Treaty of Lisbon had a direct impact on the activities and tasks of the EDPS. The Treaty assigns greater importance to data protection in the EU institutions and bodies and has thus increased the workload of the institution and in turn, of the Human Resources, Budget and Administration Unit (HRBA) as well.

The planned moderate growth of the establishment plan of the EDPS over recent years could not cope with these new tasks and responsibilities and it was necessary to hire a number of contract agents and temporary staff and to negotiate the secondment of data protection experts from other EU institutions and Data Protection Authorities in the Member States to assist the EDPS with the increasing workload.

In 2011, a more strategic and efficient management of priorities and resources was developed - particularly important in times of austerity and budgetary consolidation. A strategic review of the EDPS was launched during the year and a "Strategic Review" Task Force was set up and comprised representatives from all teams and chaired by the Director of the EDPS. An internal conference in October 2011, was an opportunity for the various EDPS teams to reflect on their respective tasks, values and objectives and to identify those of the EDPS for the years to come. This will be followed up in 2012 with an external consultation of stakeholders by means of on-line surveys, focus groups and workshops. The results will be presented at a public conference.

In 2011, the efforts to improve efficiency yielded tangible results, such as securing access to the training catalogue of the European Commission through Syslog Formation, the adoption of detailed internal manuals dealing with the recruitment of several categories of staff and a new budget implementation control mechanism which gave rise to a substantial increase in the implementation rate of the budget.

Improvements in the efficiency of the HR function will continue in 2012 when access to Sysper (personnel file management system) and MIPS (an application to coordinate missions) become available. These will facilitate some routine administrative tasks and free up resources to better position the HR team as a reliable strategic partner for the Management Board of the EDPS.

6.2. Budget

The allocated budget for the EDPS in 2011 was EUR 7 564 137. This represented an increase of 6.47% on the previous year, but taking into account the overall development of the institution and its increased workload, it represented moderate growth.

This modest budgetary rise was absorbed, in the main, by the budget line for salaries, which in monetary terms, is the most important item of the EDPS budget. A significant part of the budget was allocated to translation the of EDPS opinions on legislative proposals into all official languages. They can then be published in the *Official Journal of the*

European Union to place them in proximity to the EU legislative texts and the jurisprudence of the European Court of Justice, ensuring that the views of the EDPS can be easily located by practitioners and courts alike. Other documents adopted by the EDPS (e.g. opinions on prior checks) are translated into the working languages of the EDPS (English, French and German).

The 2010 Declaration of Assurance (DAS) from the European Court of Auditors 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 the EDPS financial data:

a) a new internal financial verification system, including check-lists for all levels of financial transactions, was introduced into the financial workflow;

b) a quarterly budget implementation report, including a line-by-line budgetary consumption follow-up, was implemented;

c) new mission forms for better control and transparency were adopted;

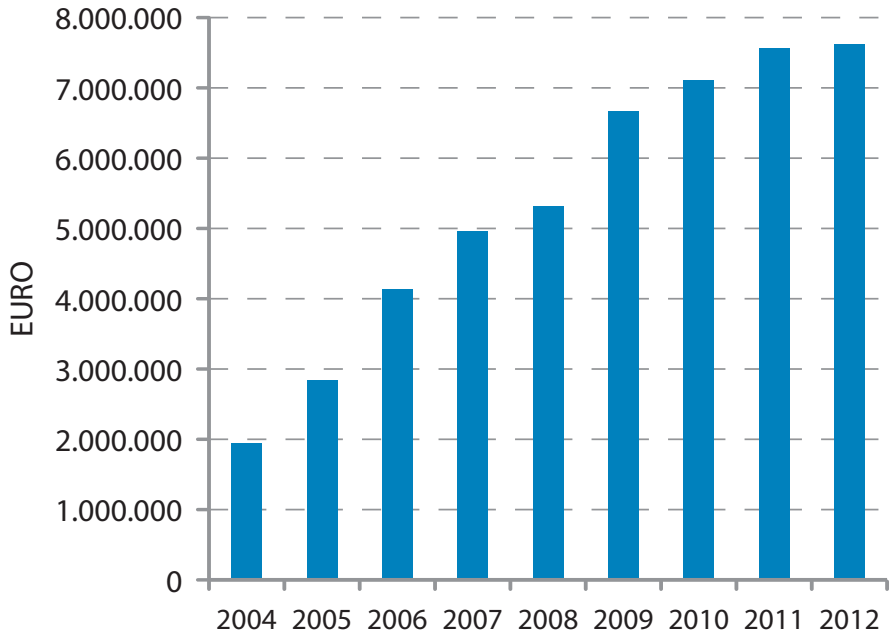
d) guidelines for low value procurements were drawn up;

e) new financial reporting tables were set up.

As a result of these initiatives, the budget implementation rate of the EDPS improved substantially: from 76% in 2010 to almost 85% in 2011.

Assistance from the European Commission in finance matters continued in 2011, particularly in relation to accountancy services - the Accounting Officer of the Commission is also the Accounting Officer of the EDPS. Where specific rules have not been laid down, the EDPS applies the internal rules of the Commission for the implementation of the budget.

EDPS - Budget evolution 2004-2012



6.3. Human resources

6.3.1. Recruitment

The growing number of tasks and increased visibility of the EDPS are leading to an increased workload and an expansion of activities which need to be addressed from a human resources perspective.

Thanks to a service level agreement with the European Personnel Selection Office (EPSO), a general competition on data protection was organised in 2009 so as to recruit highly specialised staff. Three

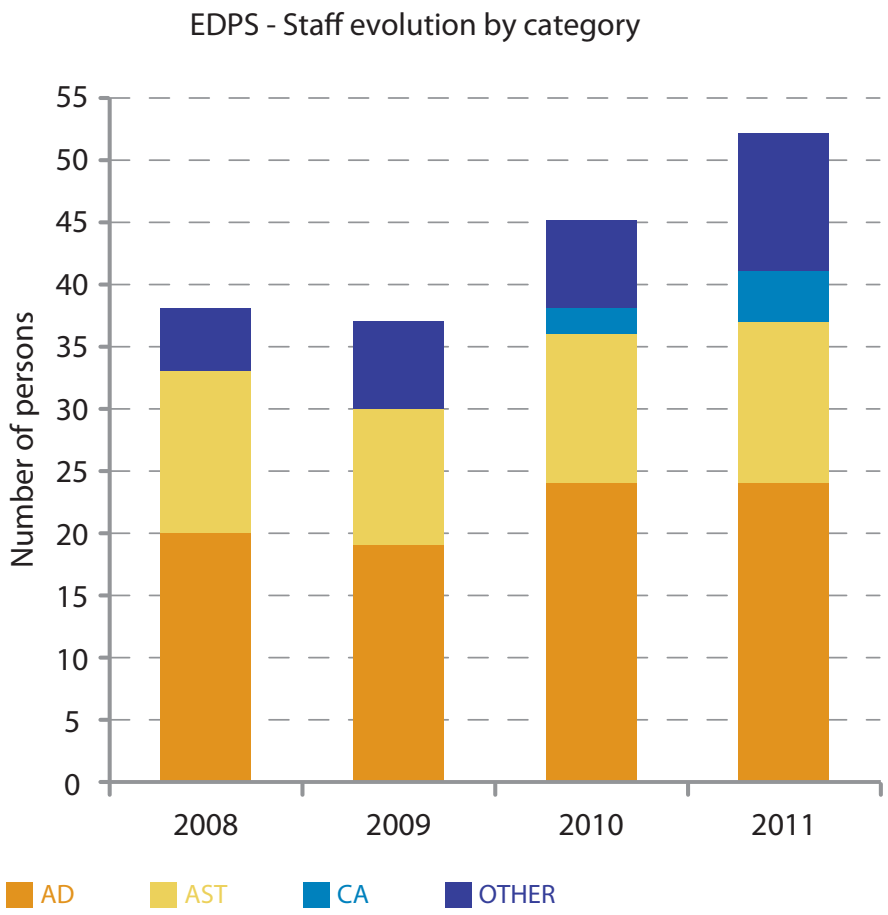
reserve lists were made available in Summer 2010 for grades AD9, AD6 and AST3 for a validity of three years. At present, 82% of the laureates on the three lists have been recruited. The AST3 list is open for recruitment by all EU institutions.

Following the publication of these lists in 2010, the EDPS embarked on a major recruitment operation, interviewing candidates from the reserve lists and officials from other institutions, in compliance with Article 29 of the Staff Regulations. This recruitment effort continued in 2011. Prior to 2011, newcomers were mainly selected from EPSO competition lists. In 2011, the EDPS began to receive 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 order to deal more efficiently with the increased number of applications and to guarantee a fair and professional recruitment process, the Human Resources team issued several recruitment manuals related to all categories of staff, setting out procedures to be followed by HR staff and line managers during the recruitment process.

In addition to officials, the EDPS recruited three contract agents and welcomed the former DPO of the Council on secondment to the EDPS, thus strengthening the Supervision Unit. In order to cover temporary needs in 2011, two interim staff members and one external contractor for the maintenance and development of the EDPS website were hired. In total, the EDPS recruited 14 new colleagues in 2011.

The procedure to fill the vacancy of Director of the EDPS Secretariat, launched at the end of 2010, was completed. Following an inter-institutional recruitment procedure, the Director was selected and appointed in March 2011.



6.3.2. Traineeship programme

A traineeship programme was created in 2005 to offer recent university graduates the opportunity to put their academic knowledge into practice, thereby acquiring practical experience in the day-to-day activities of the EDPS. This also provides the institution with an opportunity to increase its visibility among younger EU citizens, particularly among those university students and young graduates who have specialised in the field of data protection.

The programme hosts on average of 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, the EDPS may also welcome non-remunerated trainees who wish to gain experience in the field of Data Protection in the framework of their studies or professional career. The criteria are defined in the new decision that the EDPS adopted on 25 October 2011 and contains the rules governing the traineeship programme. In the new decision, particular attention is given to the data protection aspects, in order to better inform the candidates on their rights.

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

On the basis of a service level agreement with the Commission, the EDPS has benefited from the administrative assistance of the Traineeship Office of the Commission Directorate-General for Education and Culture, which has continued to provide valuable support through its highly experienced staff.

6.3.3. Programme for seconded national experts

The programme for seconded national experts (SNEs) at the EDPS was launched in January 2006. On average, two national experts from data protection authorities (DPAs) in the Member States are seconded every year. These secondments enable the EDPS to benefit from the skills and experience of such staff and help to increase the visibility of the EDPS at national level. This programme, in turn, allows SNEs to familiarise themselves with data protection issues at EU level. An internal manual governing their selection procedure was issued in 2011.

6.3.4. Organisation chart

The EDPS organisation chart remained unchanged since its inception in 2004 up to 2009, after which, the first reorganisation took place with the creation of the post of Director as Head of Secretariat.

In 2010, the EDPS organisation chart underwent a major change as the staff was reorganised into five sectors with heads of sector appointed at middle management level.

The major recruitment endeavour that followed after the publication of the EPSO competition reserve lists resulted in a substantial growth of these sectors. For this reason, in June 2011, the 3 largest EDPS sectors, namely Supervision and Enforcement, Policy and Consultation and Human Resources Budget and Administration, were transformed into units.

These changes have given rise to a new organisation chart which is available on the EDPS website.

6.3.5. Working conditions

The flexitime regime was introduced at the EDPS in 2005 and is highly appreciated by staff. Many colleagues use this opportunity to balance professional and personal life in an equitable manner.

In 2011, the decision on flexitime was revised in order to rationalise and simplify the procedure and to ensure equal treatment of all staff. Furthermore, the new decision harmonises the rules applicable at the EDPS with those in place at the European Commission, in order to facilitate the introduction of the Sysper II Time Management module in 2012.

Two staff members (one from the HR Unit and one from the Staff Committee) were appointed "trust persons" in 2011, available to all staff to discuss possible cases of harassment. The two officials followed specific training organised by the Commission to prepare them for treating possible cases and to implement a specific policy against harassment.

6.3.6. Training

Syslog Web Formation was implemented at the EDPS in 2011. This allows electronic access to the training catalogue of the European Commission and has resulted in a tremendous improvement in the efficiency and rapidity of organising training. As a consequence, most of the training budget was consumed in 2011 (88 % of the total budget – EUR 102 499).

General training courses (at the Commission, including language courses)	21.75 %
EAS training courses	48.70 %
External training courses	17.55 %

The high implementation rate of the training budget is a sign of success of the EDPS reorganisation and assists the declared objective of the Management Board of the institution to meet the needs of EDPS Staff and to make the EDPS an attractive employer for EU officials from other EU institutions.

A tailor-made "First steps in management" course was organised over 2 days by the EAS for 16 administrators from the EDPS. The course was designed to impart knowledge on management, with a focus on the basics of team management, diversity and communication. The course gave staff a better understanding of the challenges faced by middle management and prepared them for future management responsibilities. Due to its success, such a course will be organised again in 2012.

In 2011, EDPS middle management who were appointed in 2010 and 2011, followed a specific management training course and also benefited from an individual and collective coaching programme delivered by the coach coordinator of the European Commission. This has allowed the Director and the Heads of Unit and Sector to function better as individual managers and as a management team, with tangible improvements in planning, coordination and implementation of policies decided by the Management Board of the institution.

The EDPS continued to participate in various inter-institutional committees which facilitates the pooling of training needs and allows for economies of scale in an area where needs are essentially similar across the EU institutions. The sixth amendment to the protocol of language courses was signed in December 2011, an area for which there have also been a significant increase in training requests.

At the request of the training coordinator, the EDPS updated its training decision in October 2011, allowing more training opportunities to be offered to EDPS staff.

6.3.7. 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 of the EDPS. In addition to their mentor, newcomers also meet members of the HR, Budget and Administration Unit, who provide them with the EDPS administrative guide and other information on the specific procedures of the EDPS.

The EDPS has continued to develop inter-institutional cooperation with regard to 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. The EDPS also participates 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 2011, several social activities were organised for EDPS staff in close cooperation with the Staff Committee of the institution and each event resulted in a high rate of attendance.

6.4. Control functions

6.4.1. Internal control

The internal control system, effective since 2006, manages the risk of failure to achieve business objectives. In 2011, considerable efforts were put into the implementation of the Internal Control Standards (ICS). The list of actions was extended to ensure a more efficient internal control of the processes in place. By way of example, an awareness-raising action on ethics, harmonised titles for all staff, a mentorship programme, an adaptation of the new financial workflow, a business continuity plan and an update of the missions' guide were all adopted in relation to the ICS. An updated decision on Internal Control Standards will be adopted in 2012 to simplify the approach, increase the ownership and strengthen their effectiveness.

The EDPS took note of the annual activity report and the Declaration of Assurance signed by the Authorising Officer by delegation. Overall, the EDPS considers that the internal control systems in place provide reasonable assurance of the legality and regularity of operations for which he is responsible.

6.4.2. Internal audit

The Internal Audit Service (IAS) of the Commission also serves as the auditor of the EDPS. In January 2011, a risk assessment visit took place to set up the IAS audit strategy for the EDPS for the period 2011-2013. All the processes of the EDPS were thoroughly checked by the IAS and a risk map profile and trigger areas of audit visits were drawn up.

A specific IT risk assessment visit by the IAS took place at the request of the EDPS, in July 2011. As the EDPS is hosted on the premises of the European Parliament and relies on its IT infrastructure, further work with the IT services of the EP will continue in 2012.

Finally, an audit was performed in November 2011 concerning prior checking opinions, administrative measures and inspections. The report on this audit will be available in 2012.

With regard to the follow up of the 2 risk assessment audits, 6 recommendations remain open. Three of them are expected to be closed in early 2012 and the three others will be addressed later in 2012 or 2013 as they concern long-term projects such as the development of a Case Management System (see further in Section 6.6.3) or a risk management policy.

As both organisations share an interest in the area of audits, as far as compliance with data protection is concerned, the EDPS has proposed a Memorandum of Understanding to the IAS to allow both organisations to fulfil their roles in the most effective way possible. The MoU will be concluded in 2012 with full regard to their respective rights, obligations and independence as laid down in their constitutive documents.

6.4.3. 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 undertakes an annual audit of the revenue and expenditure of the EDPS in order to provide a statement of assurance as to the reliability of the 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 2010, the questions posed by the Court were answered satisfactorily by the EDPS.

6.4.4. Security

In 2011, considerable resources in the area of security were devoted to the internal Case Management System of the EPDS which will be tailor-made for the EDPS and implemented in 2012, with particular attention paid to the security measures to be put in place. The contract with the company developing the system was signed in December 2011 with the assistance of the European Parliament.

The IT risk assessment visit carried out by our internal auditor in July 2011, although not finalised, has already triggered some initiatives such as the setting up of an IT Steering Committee that met for the first time in January 2012.

The EDPS also adopted a Business Continuity Plan (BCP) in 2011 with regard to health and safety conditions for staff and premises. In 2012, following the scheduled move to new premises, a new plan will be prepared in close cooperation with other institutions.

Based on the need to access EU Classified Information (EUCI) in order to carry out their duties, several members of EDPS staff have received an official security clearance, granted by their national security authorities. This allows the EDPS to carry out security inspections of large scale IT systems or at other important and sensitive sites.

Advice was delivered on a regular basis on EDPS activities, including an introduction to the tasks and mandate of the EDPS given to the Local Security Officers (LSO) and Local Information Security Officers (LISO) of the European Commission.

6.5. Infrastructure

On the basis of the administrative cooperation agreement described below, the offices of EDPS are located in the premises of the European Parliament, which also assists the EDPS in the fields of IT and infrastructure.

Because of a recurrent lack of space in the building in which the EDPS is located and the imminent expiry of the rental contract of the building in which the EDPS is hosted (Montoyer 63), the

European Parliament set up a Building Committee, in which the EDPS participated, to select a new building to house the offices of the EDPS.

The new building was selected in 2011 and the move is planned for mid-2012. A task force named "EDPS by design" was created, with the mandate "to analyse and develop all aspects related to the design and the move to a new building (e.g. planning, space distribution, IT issues, both at short and long term perspective, security or data protection matters, etc.) in the course of 2012, so that the move is successful and disruption to the work of the Institution is reduced as much as possible."

The institution has continued to independently manage its furniture and IT goods inventory, with the assistance of the European Parliament services.

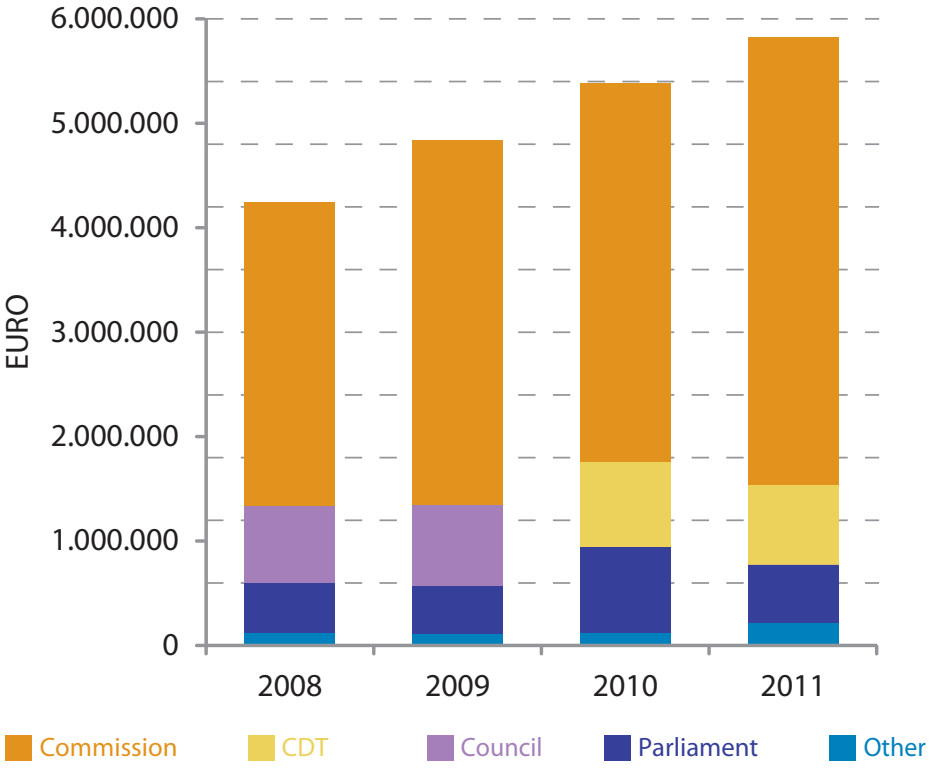
6.6. Administrative environment

6.6.1. 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 . A extension of the agreement for two-years was signed by the Secretaries-General of the Commission and the Parliament and the EDPS Director in December 2011. This cooperation is vital for the EDPS as it increases efficiency and allows for economies of scale.

Close inter-institutional cooperation continued in 2011 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 the

EDPS budget execution through inter-institutional cooperation



EDPS website; fitting out of the premises, building security, printing, mail, telephone, supplies, etc.). In many cases, this cooperation takes place by means of service level agreements, which are regularly updated. The EDPS also continued to participate in the inter-institutional calls for tenders, thus increasing efficiency in many administrative areas and making progress towards greater autonomy.

The EDPS is a member of 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*.

6.6.2. Internal rules

There was an adoption of various internal rules for the smooth functioning of the EDPS in 2011. In areas where the EDPS benefits from the assistance of the Commission or the European Parliament, the rules are similar to those of these institutions, albeit with some adjustments to allow for the specific features of the EDPS office.

In 2011, the Director's meeting (Heads of unit or sector plus Director) started discussions on adopting internal rules of a more general scope and a first proposal was submitted to the Management Board of the EDPS. The EDPS plans to adopt these in 2012 together with a revised version of the Code of good conduct for the EDPS.

6.6.3. Document management

The EDPS selected and procured a document and records management system incorporating case management. This process was completed with the support of the European Parliament IT services.

The customisation and configuration of this system to accommodate the specific needs of the EDPS began at the end of the year. The current EDPS databases have been harmonised, in preparation for migration into the new system.

6.6.4. Planning

In the course of 2011, planning and control of activities within the EDPS was improved. Three levels of planning were put in place: a strategic plan (3-5 years), an annual management plan and a detailed activity planning:

a) Strategic plan
One early outcome of the Strategic Review was to set up an accurate and detailed strategic plan. This strategic planning will allow the Management Board to manage resources more efficiently over the medium term.

b) Management plan
The annual Management Plan outlines the detailed planning for the year based on the objectives and activities mentioned in the three year strategic plan.

c) Weekly activity planning
Accurate weekly planning of activities is carried out to ensure that the EDPS meets his legal obligations and deadlines. Planning also ensures effective cooperation across the different EDPS teams.

7 EDPS DATA PROTECTION OFFICER

7.1. The DPO at the EDPS

In 2010, the DPO team consisted of two DPOs (a DPO and an assistant DPO) who had been appointed by the EDPS in September 2010. Following the departure of the DPO in March 2011, the EDPS decided to nominate the assistant DPO - who succeeded in the certification programme in 2010 - as the acting DPO. The acting DPO was nominated as DPO in December 2011, once she had been appointed to an AD post.

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 deepen her expertise, the EDPS DPO is following the IAPP (International Association of Privacy Professionals) training recommended in the DPO paper on professional standards issued by the DPO network([20]).

7.2. The Register of processing operations

2011 was dedicated to the revision of all processing operation notifications within the EDPS and to new notifications. Seven notifications were substantially revised in order to take account of the new procedures in place at the EDPS following its internal reorganisation, notably in Human Resources procedures. Eight new notifications were required, mainly in the Human Resources and Communication teams. A notification on how the EDPS deals with complaints lodged was also addressed. These notifications relate to Article 25 of Regulation 45/2011.

At the same time, the DPO has taken care of notifications submitted to the EDPS under Article 27.2 of Regulation 45/2001 following EDPS guidelines. Among the 17 existing notifications based on Article 25 of the Regulation, nine were subject to notification under Article 27 of Regulation 45/2011, of which 89% deal with Human Resources issues.

The DPO's main objective for 2012 is to request notifications of all processing operations which are in the inventory and which have not yet been established by the persons responsible for processing.

7.3. EDPS 2011 Survey

In March 2011, a letter was sent to the Supervisor by the EDPS Director outlining all the work carried out to be in compliance with Regulation 45/2001. The EDPS has taken these documents into account in his 2011 Survey. The 2010 Action Plan, which was implemented at 95%, was positively acknowledged. The EDPS underlined that all notifications under Article 27 have been completed.

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

7.4. Information and raising awareness

The DPO places great emphasis on raising awareness and on communication of data protection compliance at the EDPS, both externally and internally.

With regard to **external communication**, a DPO section of the EDPS website, which provides basic information about the DPO role and activities, has been updated, so that the updated Register and all the notifications are available for public consultation in their new versions.

In addition, the DPO takes part in the **DPO network meetings**, which represent a unique opportunity to network, discuss common problems and share best practices.

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 has been completed with a detailed list of privacy statements about the EDPS processing operations, allowing all members of staff to exercise their rights (Articles 11 and 12 of Regulation 45/2001) by informing them thereof.

Raising awareness also took the form of a DPO presentation "Initiation to Regulation 45/2001" aimed at newcomers and officials not experienced in data protection. Its purpose was to familiarise staff members with data protection matters and with the EDPS missions and values.

8 MAIN OBJECTIVES IN 2012

The following objectives have been selected for 2012. The results achieved will be reported in 2013.

8.1. Supervision and Enforcement

In line with the Compliance and Enforcement Policy Paper adopted in December 2010, the EDPS has set the following objectives in the field of Supervision and Enforcement.

- **Raising awareness**

The EDPS will invest time and resources in providing guidance to EU institutions and agencies. Guidance is necessary to help achieve a shift towards greater accountability of Institutions and agencies. This guidance will take the form of thematic papers on standard administrative procedures and horizontal themes such as e-monitoring, transfers and rights of data subjects. Training and workshops will also be organised for DPOs/DPCs either on request by a specific institution or agency or on the initiative of the EDPS when a need is identified. The EDPS website will be developed so as to provide useful information to DPOs. The public register of prior checking notifications will also be made accessible according to a common subject taxonomy.

- **Prior checking**

The EDPS continues to receive *ex-post* notifications either relating to standard administrative procedures or to processing operations already in operation. Action will be taken in 2012 to define appropriate procedures for handling such notifications and to ensure that notifications for checking *ex-post* are not permitted save in exceptional and justified circumstances. The follow-up of recommendations made in prior checking opinions is a crucial element of the enforcement strategy of the EDPS. The EDPS will continue to place strong emphasis on the implementation of recommendations in prior check opinions and ensure an adequate follow up.

- **General stock taking exercises**

In 2011, the EDPS launched a general stock taking exercise, providing indicators of compliance by institutions and bodies with certain obligations (e.g. appointment of a DPO, adoption of implementing rules, level of Article 25 notifications, level of Article 27 notifications). The report issued by the EDPS emphasised the progress made in implementing the Regulation, but also underlined shortcomings. The report will emphasise the progress made in implementing the Regulation, but will also underline shortcomings. The 2011 survey will be complemented in 2012 by a specific exercise on DPO Status: this exercise is also intended to provide support for the DPO function in line with the accountability principle. In addition, the EDPS will launch a survey specifically for the Commission in 2012, the aim of which is to collect information directly from the various DGs at the Commission.

- **Visits**

On the basis of the indicators from the 2011 survey, the EDPS has selected institutions and agencies for visits (6 planned visits). These visits are triggered

either by an apparent lack of commitment or communication from management, or if an institution or agency is below the benchmark set for a peer group.

- **Inspections**

Inspections are a vital tool that enable the EDPS to monitor and ensure the application of the Regulation: an increase in the number of inspections is crucial not only as an enforcement tool, but also as a tool to raise awareness of data protection issues and the EDPS. Inspections will increase in 2012 due to the introduction of lighter, more targeted inspections in addition to full-scale inspections. Some institutions or bodies process personal data in their core business activities and data protection is, therefore, a key element. These bodies will be identified and be the object of targeted monitoring (paper based) or inspections. General inspections are also planned for large scale IT systems in 2012. These are selected on the basis of legal obligations. Thematic inspections will be launched in areas where the EDPS has provided guidance and wishes to check against reality (e.g. CCTV).

8.2. Policy and Consultation

The main objectives of the EDPS for his advisory role are set out in the inventory and the accompanying memo as published on the website. The EDPS faces the challenge of fulfilling his ever-increasing role in the legislative procedure, guaranteeing high-quality and well-appreciated contributions to it, delivered by limited resources. In light of this, the EDPS has identified issues of strategic importance that will form the cornerstones of his consultation work for 2012, while not neglecting the importance of other legislative procedures where data protection is concerned.

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

The EDPS will give priority to the work on a new legal framework for data protection in the EU. He will issue an opinion on the legislative proposals for the framework and 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 focus for the EDPS in 2012. Subjects range from the plans for a Pan-European framework for electronic identification, authentication and signature, the issue of Internet monitoring (e.g. enforcement of IP rights, takedown procedures) to cloud computing services and eHealth. The EDPS will also strengthen his technological expertise and engage in research on privacy-enhancing technologies.

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

The Area of Freedom, Security and Justice will remain one of the key policy areas for the EDPS to address. Relevant upcoming proposals include EU-TFTS and smart borders. Additionally, the EDPS will continue to follow the review of the data retention directive. He will also closely monitor negotiations with third countries on data protection agreements.

- **Financial sector reform**

The EDPS 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.

- **Other initiatives**

The EDPS will also follow proposals in other policy areas that have a significant impact on data protection. He will continue to be available for formal and informal consultations on proposals affecting the right to privacy and data protection.

8.3. Cooperation

The EDPS will continue to fulfil his responsibilities in the field of coordinated supervision. Additionally, he will reach out to national data protection authorities as well as to international organisations.

- **Coordinated supervision**

The EDPS will play his role in the coordinated supervision of Eurodac, the Customs Information System and the Visa Information System (VIS). Coordinated supervision of the VIS, which went live in October 2011, is still in its infancy. After informal discussions in the framework of the Eurodac supervision coordination meetings, the target for 2012 is to gradually establish supervision in this area. When SIS II is launched, it will also be subject to coordinated supervision; it is scheduled to go live

in 2013 and the preparations will be followed closely. The EDPS will also carry out inspections of the central units of these systems where necessary or legally required.

- **Cooperation with data protection authorities**

As before, the EDPS will actively contribute to the activities and success of the Article 29 Data Protection Working Party, ensuring consistency and synergies between the Working Party and the positions of the EDPS in line with respective priorities and maintaining a constructive relationship with national data protection authorities. As *rapporteur* for some specific dossiers, he will steer and prepare the adoption of WP29 opinions.

- **Data protection in international organisations**

International organisations are usually not subject to data protection legislation in their host countries; however, not all of them have appropriate rules for data protection in place. The EDPS will reach out to international organisations by organising a workshop aimed at raising awareness and spreading good practices.

8.4. Other fields

- **Information and communication**

Information, communication and press activities will continue to be developed and improved, with special focus on awareness-raising, publications and online information. The EDPS will also start implementing the review of his Information and Communication Strategy, after the consultation of his main stakeholders. The re-organisation of some important parts of the EDPS website is planned in order to increase the user friendly character of the website and facilitate search and navigation through the available information.

- **Internal organisation**

The EDPS strategic review will continue through 2012, with an external consultation of stakeholders by means of online surveys, interviews, focus groups and workshops. Immediate results of the review launched in 2011 led to decisions to develop a more strategic approach to supervision and consultation activities and to create a new IT policy sector in 2012. Once the review has been concluded and the results analysed, the EDPS will finalise his mid-term strategy and draw up the performance measuring tools (KPI) necessary to evaluate key elements of that strategy.

- **Resource management**

The work of developing a customised Case Management System at the EDPS will continue in 2012. IT applications in the field of human resources on the basis of Service Level Agreements will also be developed further, especially with the implementation of Sysper II, which will be completed in 2012, and with the introduction of MIPS.

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 ([21]).

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 are still being examined and may require further clarification.

The definitions and the substance of the Regulation closely follow the approach of Directive 95/46/EC. It could be said that Regulation (EC) No 45/2001 is the implementation of that directive at European level. This means that the Regulation deals with general principles like fair and lawful processing, proportionality and compatible use, special categories of

([21]) OJ L 8, 12.1.2001, p. 1.

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. This means that important work has been done to implement the Regulation, even in the absence of a supervisory body. These officers may also be 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)	Jonathan STEELE	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)	Jean-Philippe MINNAERT	Dataprotectionofficer@eib.org
European External Action Service (EEAS)	Ingrid HVASS	Ingrid.HVASS@eeas.europa.eu
European Ombudsman	Loïc JULIEN	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)	Ignacio DE MEDRANO CABALLERO	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)	Eusebio RIAL GONZALES	rial@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	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)	Alain LEFÈBVRE	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
European Systemic Risk Board (ESRB)	Frederik MALFRÈRE	DPO@ecb.int

>>>

ORGANISATION	NAME	E-MAIL
Fusion for Energy	Radoslav HANAK	Radoslav.Hanak@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	Silvia POLIDORI	Silvia.Polidori@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	leelo.kilg@cepol.europa.eu
European Institute of Innovation and Technology (EIT)	Roberta MAGGIO	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

Annex E — List of prior check opinions

Procurement procedures - CFCA

Opinion of 21 December 2011 on the notification for prior checking concerning procurement procedures at the Community Fisheries Control Agency (Case 2011-0890)

Video-surveillance system - ECA

Letter of 20 December 2011 on the notification for prior checking regarding the video-surveillance system at the European Court of Auditors (ECA) (Case 2011-0989)

360° feedback survey for managers

Opinion of 20 December 2011 on a notification for prior checking regarding the "360° feedback survey for managers" at the Committee of the Regions (Case 2011-0926)

Staff Evaluation Procedures - Eurofound

Opinion of 19 December 2011 on the notification for prior checking regarding probationary reports, staff appraisals and promotions at the European Foundation for Improvement of Living and Working Conditions (Case 2011-0628)

Interventions of the Chambre d'écoute in the Framework of the Reorganization of OLAF's Organigram

Opinion of 16 December 2011 on the notification for prior checking regarding Interventions of the Chambre d'écoute in the Framework of the Reorganization of OLAF's Organigram (case 2011-1021)

Procédure relative aux commissions d'invalidité - Cour de Justice

Avis du 15 décembre 2011 sur la notification d'un contrôle préalable à propos du dossier "Procédure relative aux commissions d'invalidité" (Dossier 2011-0655)

Staff evaluation procedures - European Chemicals Agency

Opinion of 15 December 2011 on the notificaton for prior checking regarding staff evaluation procedures at the European chemicals Agency (ECHA) (Case 2011-0945)

Staff appraisals - ACER

Opinion of 15 December 2011 on the notification for prior checking concerning Probationary Reports and Staff appraisals including appraisal of Director at the Agency for the cooperation of Energy Regulators (ACER) (Case 2011-0953)

Probationary reports, staff appraisals, reclassification - ERCEA

Opinion of 15 December 2011 on the notification for prior checking concerning the annual appraisal and probation, reclassification and assessment of the ability to work in a third language at the European Research Council Executive Agency (Case 2011-0955/0956/0963)

Staff evaluation procedures - Trans-European Transport Network Executive Agency

Joint Opinion of 14 December 2011 on the notifications for prior checking regarding staff evaluation procedures at the Trans-European Transport Network Executive Agency (TEN-T EA) (case 2011-0990)

Procedure for early retirement without reduction of pension rights - CPVO

Opinion of 13 December 2011 on the notification for prior checking on the procedure for early retirement without reduction of pension rights at the Community Plant Variety Office (CPVO) (Case 2011-0304)

Transmission of inspection reports - CFCA

Joint opinion of 30 November 2011 on two notifications for Prior Checking concerning the "Transmission of inspection reports related to the bluefin tuna joint deployment plan (BFT JDP) and transmission of inspection reports (NAFO/NEAFC)", Community Fisheries Control Agency (CFCA) (Cases 2011-0615 and 2011-0636)

Procurement procedures and related procurement contracts - CPVO

Opinion of 30 November 2011 on the notification for prior checking concerning procurement procedures and related procurement contracts at the Community Plant Variety Office (Case 2011-0740)

E-recruitment for the Graduate Recruitment and Development Programme - EIB

Letter of 24 November 2011 on notification for prior checking regarding "E-recruitment for the Graduate Recruitment and Development Programme" at the European Investment Bank (Case 2009-0761)

Selection of experts - ERA

Opinion of 22 November 2011 on the notifications for prior checking concerning the Calls for applications to establish lists of prospective independent experts to assist the work of the Working Parties/Groups/Task Forces of the European Railway Agency in the fields of Railway Safety and Railway Interoperability (Joint Cases 2011-0667/0668)

Evaluation and grants management - ERCEA

Opinion of 21 November 2011 on the notification for prior checking concerning proposals evaluation and grants management at the European Research Council Executive Agency (ERCEA) (Case 2011-0845)

Recruitment of staff and selection and recruitment of trainees - Fuel Cells Hydrogen Joint Undertaking

Opinion of 15 November 2011 on the notifications for prior checking concerning selection and recruitment of staff and selection and recruitment of trainees, Fuel Cells Hydrogen Joint Undertaking (FCH JU) (Cases 2011- 0833/0834)

Procédures de sélection des agents contractuels - Commission européenne

Lettre du 11 novembre 2011 sur la notification d'un contrôle préalable concernant des procédures de sélection des agents contractuels dans les services de la Commission européenne (Dossier 2011-0820)

Video-surveillance system - ECHA

Letter of 25 October 2011 on notification for prior checking on the video-surveillance system at the European Chemicals Agency (ECHA) (Case 2011-0012)

"Return to Work" policy - EU-OSHA

Opinion of 24 October 2011 on a notification for prior checking regarding the policy "Return to Work" at the European Agency for Safety and Health at Work (EU-OSHA) (Case 2011-0752)

Selection of confidential counsellors and anti-harassment policy

Opinion of 21 October 2011 on notifications for prior checking concerning the "anti-harassment policy" and "the selection of confidential counsellors" at certain EU agencies (Case 2011-0483)

Recrutement du personnel - Cour de justice

Lettre du 21 octobre 2011 sur la notification d'un contrôle préalable des traitements de données relatifs au "recrutement du personnel" au Cour de justice de l'Union européenne (Dossier 2011-0388)

Probation at the CPVO

Opinion of 19 October 2011 on a notification for prior checking concerning assessment and reporting on probationary period at the Community Plant Variety Office (Case 2011-0298)

Virtual Operational Cooperation Unit, the Mutual Assistance Broker, and the Customs Information System - OLAF

Joint opinion of 17 October 2011 on notifications for prior checking regarding the Virtual Operational Cooperation Unit, the Mutual Assistance Broker, and the Customs Information System (Joint cases 2010-0797/0798/0799)

Selection of participants to (internal/external) learning and development actions - EC

Opinion of 17 October 2011 on the notification for prior checking concerning "Selection of participants to (internal/external) learning and development actions" (Case 2011-0627)

Internal mobility of staff members - EACEA

Opinion of 17 October 2011 on the notification for prior checking concerning "internal mobility of EACEA's staff members" (Case 2011-0672)

Electronic CV

Opinion of 4 October 2011 on the notification for prior checking from the Data Protection Officer of the European Parliament concerning Electronic CV (Case 2011-0568)

Selection procedure for the position of Member of the Management Board - EFSA

Opinion of 3 October 2011 on a notification for prior checking regarding the "Selection procedure for the position of Member of the Management Board of the European Food Safety Authority (EFSA)" (Case 2011-0575)

Selection and recruitment of SNEs, trainees and temporary staff - Eurofound

Opinion of 27 September 2011 on a notification for prior checking on the selection and recruitment of SNEs, trainees and temporary staff (Cases 2011-0645/0646/0647)

PMO - establishment of individual output indicators

Opinion of 23 September 2011 on the notification for prior checking concerning the establishment of individual output indicators (Case 2011-0368)

DG INFSO Staff Competencies and Aspirations Mapping Database

Opinion of 23 September 2011 on a notification for prior checking concerning DG INFSO Staff Competencies and Aspirations Mapping Database (Case 2011-0614)

"IDEAS-Exclusion of Experts by Applicants" project - ERCEA

Opinion of 21 September 2011 on a notification for prior checking regarding the project "IDEAS-Exclusion of Experts by Applicants" of the European Research Council Executive Agency (ERCEA) (Case 2010-0661)

Establishment and payment of salaries and allowances

Opinion of 19 September 2011 on the processing of personal data by the services of the European Foundation for the Improvement of Living and Working Conditions (Eurofound) for the "establishment and payment of salaries and allowances" (Case 2011-0644)

Administrative inquiries and disciplinary proceedings - Court of Justice

Opinion of 12 September 2011 on the updated notification concerning administrative inquiries and disciplinary proceedings within the Court of Justice of the EU (Case 2011-0806)

Further development of DG Translation managers

Opinion of 9 September 2011 on the notification for prior checking concerning Feedback for further development of DG Translation managers (Case 2011-0511)

Selection and recruitment of SNEs at Fusion for Energy

Opinion of 9 September 2011 on the notifications for prior checking on the processing operations related to the selection and recruitment of SNEs at Fusion for Energy (F4E) (Case 2011-0340)

Seconded National Experts

Letter of 9 September 2011 on the notification for prior checking on processing of data in connection with 'Seconded National Experts' (SNEs) (Case 2011-0557)

Commission Physical Access Control System (PACS)

Opinion of 8 September 2011 on the "Commission Physical Access Control System (PACS): PSG Projet de Sécurisation Globale" (Case 2010-0427)

Selection procedure for temporary agents

Opinion of 29 July 2011 on a notification for prior checking on the processing operations related to the selection procedure for temporary agents organised by the European Commission (EC) for "posts other than supervision and advice without EPSO concours" (Case 2011-0559)

Electronic Exchange of Social Security Information system

Opinion of 28 July 2011 on a notification for prior checking on the Electronic Exchange of Social Security Information system ("EESSI") (Case 2011-0016)

Requests for a part-time work - CPVO

Opinion of 28 July 2011 on a notification for prior checking regarding requests for a part-time work at the Community Plant Variety Office (Case 2011-0299)

Mobility Procedure

Opinion of 27 July 2011 on the notification for prior checking relating to the 'Mobility Procedure' (Case 2011-0648)

Executive Committee and the Technical Advisory Panel of the Fusion for Energy

Opinion of 26 July 2011 on the notifications for prior checking from the Data Protection Officer of Fusion for Energy concerning the calls for expression of interest for external experts to be appointed to the Executive Committee and the Technical Advisory Panel of the Fusion for Energy (Joint Cases 2011-0363/0364)

Fingerprint recognition study of children below the age of 12 years

Opinion of 25 July 2011 on a notification for prior checking related to the "Fingerprint recognition study of children below the age of 12 years" (Case 2011-0209)

Management of the European Parliament's Crèches in Brussels

Opinion of 25 July 2011 on the notification for prior checking on the "Management of the European Parliament's Crèches in Brussels" (Case 2010-0385)

Access Control System

Opinion of 15 July 2011 on a notification for prior checking on Access Control System at JRC Ispra Site (Case 2010-0902)

Processing of administrative inquiries and disciplinary proceedings - EASA

Letter of 13 July 2011 on the notification for prior checking concerning the processing of administrative inquiries and disciplinary proceedings (the AI&DP) at the European Aviation Safety Agency (EASA) in the light of the EDPS Guidelines on AI&DP (Case 2011-0558)

Sickness Leave at OHIM

Opinion of 12 July 2011 on the notification for prior checking concerning Control and Management of Sickness Leave at the Office for Harmonisation of the Internal Market (Case 2010-0263)

Agents intérimaires - Comité des régions

Lettre du 30 juin 2011 sur la notification d'un contrôle préalable concernant des traitements de données relatifs aux agents intérimaires au Comité des régions (Dossier 2010-0796)

Processing of administrative inquiries and disciplinary proceedings

Opinion of 22 June 2011 on notifications for prior checking regarding the "processing of administrative inquiries and disciplinary proceedings" in certain EU agencies (Case 2010-0752)

Quality Management System and ex-post quality checks - OHIM

Opinion of 9 June 2011 on the notification for prior regarding Quality Management System and ex-post quality checks for Harmonization at the Office for Harmonization for the Internal Market ("OHIM") (Case 2010-0869)

Selection of trainees - CPVO

Letter of 1 June 2011 on a notification for prior checking on the processing of data in connection with the selection of trainees at the CPVO (Case 2011-0214)

Selection procedure of SNEs - JRC

Opinion of 30 May 2011 on the notification for prior checking regarding the "Selection procedure of SNEs at JRC" (Case 2008-0141)

Staff Appraisal at CEDEFOP

Opinion of 24 May 2011 on the notification for prior checking concerning Staff Appraisal at the European Centre for the Development of Vocational Training (Case 2010-0620)

Certification procedure - CPVO

Opinion of 19 May 2011 on the notification for prior checking concerning the certification procedure at the Community Plant Variety Office (Case 2011-0055)

Consumer Protection Co-operation System (CPCS)

Opinion of 4 May 2011 on the notificatin for prior checking concerning the Consumer Protection Co-operation System ("CPCS") (Case 2009-0019)

Procurement procedures - EACEA

Opinion of 29 April 2011 on the notification for prior checking concerning procurement procedures at the Education Audiovisual and Culture Executive Agency (EACEA) (Case 2011-0135)

Grant and procurement award procedures including call for expression of interest - EEA

Opinion of 18 April 2011 on the notification for prior checking concerning 'Grant and procurement award procedures including call for expression of interest' at the European Environment Agency (Case 2011-0103)

Selection of the members of the European Systemic Risk Board Advisory Scientific Committee - ECB

Opinion of 13 April 2011 on a notification for prior checking regarding the "Selection of the members of the European Systemic Risk Board Advisory Scientific Committee" at the European Central Bank (Case 2011-0101)

"Anti-harassment policy and the setting up of an interagency network of confidential counsellors" and "the selection of confidential counsellors"

Opinion of 11 April 2011 on notifications for prior checking concerning the "anti-harassment policy and the setting up of an interagency network of confidential counsellors" and "the selection of confidential counsellors" (Case 2011-0151)

Selection and recruitment of officials, temporary and contracts agent - F4E

Letter of 7 April 2011 on a notification for prior checking concerning selection and recruitment of officials, temporary and contracts agent at the Fusion for Energy (F4E) (Case 2010-0454)

"Management of leave" and "Management of Leave on Personal Grounds and Unpaid Leave" - CPVO

Joint opinion of 28 March 2011 on two notifications for prior checking concerning "Management of leave" and "Management of Leave on Personal Grounds and Unpaid Leave" at the Community Plant Variety Office (CPVO) (Cases 2010-0073/0075)

Selection and Appointment of members of EFSA's Scientific Committee and Panels - EFSA

Opinion of 21 March 2011 on the notification for prior checking regarding the "Selection and Appointment of members of EFSA's Scientific Committee and Panels" (Case 2010-0980)

Management of Recruitment Files for Temporary Agents - JRC

Opinion of 9 March 2011 on a notification for prior checking regarding the Management of Recruitment Files for Temporary Agents at the Joint Research Centre (JRC) (Case 2008-0143)

Analytical accounting and performance reports - OHIM

Opinion of 2 March 2011 on a notification for prior checking regarding "Analytical accounting and performance reports" (Case 2009-0771)

Processing of data in connection with the selection and recruitment of trainees - ERA

Letter of 2 March 2011 on the notification for prior checking concerning the processing of data in connection with the selection and recruitment of trainees at the ERA (Case 2010-0313)

CRIS-Follow up of experts availability in FWC assignment - EC

Opinion of 23 February 2011 on a notification for prior checking regarding "CRIS-Follow up of experts availability in FWC assignment" (Case 2010-0465)

Processing of health data in the workplace

Opinion of 11 February 2011 on notifications for prior checking concerning the "processing of health data in the workplace" (Case 2010-0071)

Processing operations "Listening Points/ Informal procedures" - EMA

Opinion of 7 February 2011 on a notification for prior checking regarding the processing operations "Listening Points/Informal procedures" (management of cases of psychological or sexual harassment) (Case 2010-0598)

Evaluation of the EMCDDA Director

Opinion of 26 January 2011 on the notification for prior checking concerning Probationary Period, Management Probationary Period and Annual Performance Appraisal of the Director of the European Monitoring Centre for Drugs and Drug Addiction (case 2010-0895)

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

Opinions on legislative proposals

Common Agricultural Policy after 2013

Opinion of 14 December 2011 on the legal proposals for the Common Agricultural Policy after 2013

Use and transfer of Passenger Name Records to the United States Department of Homeland Security

Opinion of 9 December 2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security

Internal Market Information System ('IMI')

Opinion of 22 November 2011 on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')

Community control system for ensuring compliance with the rules of the Common Fisheries Policy

Opinion of 28 October 2011 on the Commission Implementing Regulation (EU) No 404/2011 of 8 April 2011 laying down detailed rules for the implementation of Council Regulation (EC) No 1224/2009 establishing a Community control system for ensuring compliance with the rules of the Common Fisheries Policy

Legislative package on the victims of crime

Opinion of 17 October 2011 on the legislative package on the victims of crime, including a proposal for a Directive establishing minimum standards on the rights, support and protection of the victims of crime and a proposal for a Regulation on mutual recognition of protection measures in civil matters

European Account Preservation Order

Opinion of 13 October 2011 on a proposal for a Regulation of the European Parliament and of the Council creating a European Account Preservation Order to facilitate cross-border debt recovery in civil and commercial matters

Customs enforcement of intellectual property rights

Opinion of 12 October 2011 on the proposal for a Regulation of the European Parliament and of the Council concerning customs enforcement of intellectual property rights

Net neutrality

Opinion of 7 October 2011 on net neutrality, traffic management and the protection of privacy and personal data

Recording equipment in road transport

Opinion of 5 October 2011 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and the Council

European statistics on safety from crime

Opinion of 19 September 2011 on the Proposal for a Regulation of the European Parliament and of the Council on European statistics on safety from crime

Credit agreements relating to residential property

Opinion of 25 July 2011 on the proposal for a Directive of the European Parliament and of the Council on credit agreements relating to residential property

PNR - Australia

Opinion of 15 July 2011 on the Proposal for a Council Decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service

Migration

Opinion of 7 July 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration

Technical requirements for credit transfers and direct debits in euros

Opinion of 23 June 2011 on the Proposal for a Regulation of the European Parliament and of the Council establishing technical requirements for credit transfers and direct debits in euros and amending Regulation (EC) No 924/2009

Energy market integrity and transparency

Opinion of 21 June 2011 on the Proposal for a Regulation of the European Parliament and of the Council on energy market integrity and transparency

Investigations conducted by the European Anti-Fraud Office (OLAF)

Opinion of 1 June 2011 on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EURATOM) No 1074/1999

Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)

Opinion of 31 May 2011 on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)

Interconnection of central, commercial and companies registers

Opinion of 6 May 2011 on the Proposal for a Directive of the European Parliament and of the Council amending Directives 89/666/EEC, 2005/56/EC and 2009/101/EC as regards the interconnection of central, commercial and companies registers

Consumer Protection Cooperation System ("CPCS")

Opinion of 5 May 2011 on the Consumer Protection Cooperation System ("CPCS") and on Commission Recommendation 2011/136/EU on guidelines for the implementation of data protection rules in the CPCS

OTC derivatives, central counterparties and trade repositories

Opinion of 19 April 2011 on the proposal for a Regulation of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories

Financial rules applicable to the annual budget of the Union

Opinion of 15 April 2011 on the proposal for a Regulation of the European Parliament and of the Council on the financial rules applicable to the annual budget of the Union

Passenger Name Record

Opinion of 25 March 2011 on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Turbine (TrUsted Revocable Biometric IdeNtitiEs)

Opinion of 1 February 2011 on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)

Comprehensive approach on personal data protection in the European Union

Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union"

Formal comments on legislative proposals

Amended proposal on OLAF Regulation No 1073/1999

Letter of 19 December 2011 concerning a new Article and recital in the amended proposal on OLAF Regulation No 1073/1999

Rights and Citizenship Programme

Letter of 19 December 2011 on the Proposal for a Regulation of the European Parliament and of the Council establishing for the period 2014 to 2020 the Rights and Citizenship Programme

Implementation of the harmonised EU-wide in-vehicle emergency call ("eCall")

EDPS comments of 12 December 2011 on the Commission Recommendation and the accompanying impact assessment on the implementation

of the harmonised EU-wide in-vehicle emergency call ("eCall")

EDPS comments on various legislative proposals concerning certain restrictive measures with regard to Afghanistan, Syria and Burma/Myanmar

Letter of 9 December 2011 to the President of the Council of the European Union on various legislative proposals concerning certain restrictive measures with regard to Afghanistan, Syria and Burma/Myanmar

EDPS comments on a proposal for a Directive on energy efficiency

Letter of 27 October 2011 to Mr Günther H. Oettinger, Commissioner for Energy on a proposal for a Directive of the European Parliament and of the Council on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC

Terrorist Finance Tracking System (TFTS)

Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 13 July 2011: "A European terrorist finance tracking system: Available options"

Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law

EDPS comments of 24 of October 2011 on the Communication of European Commission 'Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law'

Common basic standards on civil aviation security

Comments of 17 October 2011 on the draft proposals for a Commission Regulation and for a Commission implementing Regulation on common basic standards on civil aviation security as regards the use of security scanners at EU airports

Commentaires du CEPD sur la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale

Letter of 20 September 2011 to Ms Viviane Reding, Vice-President of the European Commission on a proposal for a Regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

EDPS comments on the Anti-Corruption Package

EDPS letter of 6 July 2011 on the Commission's Communication "Fighting Corruption in the EU" and the Commission Decision establishing an EU Anti-corruption reporting mechanism for periodic assessment

Intellectual Property Rights Directive

EDPS response of 8 April 2011 to the Commission's Consultation on its Report on the application of Intellectual Property Rights Directive

Various legislative proposals concerning certain restrictive measures, with regard to Iran, in the Republic of Guinea-Bissau, in Côte d'Ivoire, in Belarus, in Tunisia, in Libya and in Egypt

EDPS letter of 16 March 2011 concerning various legislative proposals concerning certain restrictive measures, with regard to Iran, in the Republic of Guinea-Bissau, in Côte d'Ivoire, in Belarus, in Tunisia, in Libya and in Egypt.

Annex G — Speeches by the Supervisor and Assistant Supervisor in 2011

The Supervisor and the Assistant Supervisor continued in 2011 to invest substantial time and effort in explaining their mission and raising awareness of data protection in general, as well as a number of specific issues in speeches and similar contributions for different institutions and in various Member States throughout the year.

European Parliament

12 January	Supervisor, JURI Committee, WG on Administrative Law (Brussels)
26 January	Supervisor, JURI Committee about sensitive data on Internet (Brussels)
14 March	Assistant Supervisor, ITRE Committee on draft Regulation on ENISA (Brussels)
31 March	Supervisor, ETICA - Ethics and Governance of Future and Emerging ICTs (Brussels) (*)
13 April	Supervisor, LIBE Committee on Public access to documents (Brussels) (*)
27 April	Supervisor, JURI Conference on Administrative Law (Leon)
15 June	Supervisor and Assistant Supervisor, LIBE Committee on Annual Report 2010 (Brussels) (**)
4 October	Supervisor, LIBE Committee on Cyber Attacks against Information Systems (Brussels) (*)
10 November	Supervisor, LIBE Committee on EU Charter of Fundamental Rights (Brussels) (*)

Council

17 January	Supervisor, WP on Data Protection and Information Exchange (Brussels)
27 January	Supervisor, Polish Permanent Representation on Data Protection Day (Brussels)
1 March	Assistant Supervisor, WP on ENISA Regulation (Brussels) (*)
4 May	Assistant Supervisor, WP on Data Protection and Information Exchange (Brussels) (*)
16 June	Supervisor and Assistant Supervisor, International DP Conference (Budapest) (*)
23 June	Assistant Supervisor, WP on General Matters on EU PNR (Brussels)
21 September	Supervisor, International Data Protection Conference (Warsaw)
18 November	Assistant Supervisor, Ministerial Conference on e-Government (Poznan) (*)
23 November	Assistant Supervisor, WP on Statistics on Safety for Crime (Brussels) (*)

European Commission

28 January	Supervisor, Joint High Level Meeting on Data Protection (Brussels) (*)
22 June	Supervisor, Conference on Data Retention (Brussels)
22 June	Assistant Supervisor, European Group of Ethics (EGE) (Brussels)
15 September	Supervisor, Secretary-General and Directors-General
28 September	Assistant Supervisor, EC-Etsi on Standards in the Cloud (*)
20 October	Assistant Supervisor, Sixth Security Symposium (Brussels) (*)

Other EU institutions and bodies

11 January	Assistant Supervisor, European Economic and Social Committee (Brussels)
28 January	Supervisor and Assistant Supervisor, Data Protection Day (Brussels) (**)

7 February	Supervisor, European Administrative School, Erasmus (Brussels)
9 February	Assistant Supervisor, European Economic and Social Committee (Brussels) (*)
28 March	Supervisor, European Administrative School, Erasmus (Brussels)
8 June	Assistant Supervisor, Data Protection Officers Workshop (Brussels)
13 October	Supervisor, Heads of European Agencies (Helsinki)
20 October	Assistant Supervisor, European Administrative School, Erasmus (Brussels)

International Conferences

27 January	Supervisor, Computers, Privacy & Data Protection (Brussels)
27 January	Assistant Supervisor, Computers, Privacy & Data Protection (Brussels) (*)
10 March	Supervisor, IAPP Global Privacy Summit (Washington DC)
5 April	Supervisor and Assistant Supervisor, European Data Protection Authorities (Brussels)
12 July	Supervisor, Privacy Laws & Business (Cambridge)
1 November	Supervisor and Assistant Supervisor, Privacy and Data Protection Commissioners (Mexico City)
21 November	Assistant Supervisor, Council of Europe on Rights of the Child 2012-2015 (Monaco) (*)
30 November	Supervisor, IAPP Europe (Paris)
2 December	Assistant Supervisor, UN-ISPAC and CNPDS on Cybercryme (Courmayeur) (*)
6 December	Supervisor, EU Data Protection & Privacy (Brussels)

Other events

19 January	Supervisor, Boltzmann Institute for Human Rights (Vienna)
26 January	Supervisor, GSM Association (Brussels)
3 February	Assistant Supervisor, FIDE Forum on Data Protection in the EU (Madrid)
10 February	Supervisor, European Policy Centre (Brussels)
11 February	Supervisor, University of Leuven, Faculty of Law (Leuven)
17 February	Supervisor, Centre for European Policy Studies (Brussels)
21 February	Supervisor, Senate of Dutch Parliament (The Hague)
23 February	Supervisor, Internet Society / INET Conference (Frankfurt) (**)
24 February	Supervisor, Data Protection Conference (Edinburgh)
24 February	Assistant Supervisor, CRID Workshop on Cloud Computing (Brussels)
2 March	Supervisor, IT Security and e-Privacy (Copenhagen)
21 March	Assistant Supervisor, Justice and Protection of Citizens (Brussels)
23 March	Supervisor, Workshop Privacy Principles (Copenhagen)
24 March	Supervisor, Saxony Office Expert Seminar on e-Justice (Brussels) (*)
29 March	Assistant Supervisor, EUROISPA Digital Roundtable (Brussels)
30 March	Supervisor, Hearing Italian Chamber of Deputies (Rome) (*)
8 April	Assistant Supervisor, IT Cassation Court on Penal Law and Internet (Rome)

14 April	Supervisor, Computers & Data Protection Forum (Copenhagen)
3 May	Supervisor, Council of Europe on Public Access (Brussels)
5 May	Supervisor, C-PET on EU-US relations (Washington DC)
6 May	Supervisor, RISE Conference on Biometrics (Washington DC)
9 May	Assistant Supervisor, Rome University on Fundamental Rights in the EU (Rome)
12 May	Supervisor, Clyde & Co Seminar on Data Protection (London)
12 May	Assistant Supervisor, European Banking Forum (Brussels)
17 May	Supervisor, European Data Protection Day (Berlin)
20 May	Assistant Supervisor, AIDP on Privacy in the Workplace (Cagliari)
25 May	Assistant Supervisor, Accountability Phase III (Madrid)
26 May	Assistant Supervisor, ISMS Forum on Cross Border Data Flows (Madrid)
26 May	Supervisor, Biometrics Institute Australia (Sydney) (*) and (**)
27 May	Supervisor, Data Protection Intensive (London)
8 June	Assistant Supervisor, PSC Europe Forum Conference on Videosurveillance (Brussels) (*)
15 June	Supervisor, European Biometrics Seminar (Brussels)
28 June	Supervisor, Internet of Things (Brussels)
5-6 July	Assistant Supervisor, Consent Social Networking Summit (Göttingen) (*)
7 July	Supervisor, University of Edinburgh, School of Law (*)
19 September	Supervisor, FD Blueprint on Data Protection Review (Brussels)
20 September	Supervisor, Media Law and Data Protection (London)
27 September	Supervisor, 10th Anniversary EPOF (Brussels)
28 September	Supervisor, RIM Information Security (Berlin)
29 September	Supervisor, Centre for European Reform (Brussels)
4 October	Supervisor, Lisbon Council Digital Agenda Summit (Brussels)
28 October	Supervisor, Data Protection in Criminal Process (Madrid)
9 November	Supervisor, NAID-ARMA Conference (London)
18 November	Assistant Supervisor, Lobbying, Transparency and EU institutions (Brussels)
25 November	Supervisor, Privacy Impact Assessment Conference (Berlin)
10 December	Supervisor, Felix Meritis, Bescherming Burgerrechten (Amsterdam)

(*) 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*
Laurent BESLAY (*) *Coordinator for Security and Technology*	Jaroslaw LOTARSKI *Coordinator for Complaints*
Maria Verónica PEREZ ASINARI *Coordinator for Consultations*	Athena BOURKA *Seconded National Expert*
Bart DE SCHUITENEER *Technology Officer* *Local Security Officer/LISO*	Raffaele DI GIOVANNI BEZZI *Legal Officer*
Elisabeth DUHR *Seconded National Expert*	Delphine HAROU *Legal Officer*
John-Pierre LAMB (*) *Seconded National Expert*	Ute KALLENBERGER *Legal Officer*
Xanthi KAPSOSIDERI *Legal Officer*	Luisa PALLA *Supervision and Enforcement Assistant*
Dario ROSSI *Supervision and Enforcement Assistant* *Accounting Correspondent* *External Data Warehouse Manager (EDWM)*	Galina SAMARAS *Supervision and Enforcement Assistant*
Tereza STRUNCOVA *Legal Officer*	Michaël VANFLETEREN *Legal Officer*

• Policy and Consultation

Hielke HIJMANS *Head of Unit*	Bénédicte HAVELANGE (*) *Coordinator for Large Scale IT Systems and Border Policy*
Herke KRANENBORG *Coordinator for Court Proceedings*	Anne-Christine LACOSTE *Coordinator for cooperation with DPAs*
Rosa BARCELO (*) *Legal Officer*	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 / Contract Agent*	Per JOHANSSON *Legal Officer*
Owe LANGFELDT *Legal Officer / Interim*	Roberto LATTANZI (*) *Seconded National Expert*
Parminder MUDHAR *Policy and Consultation Assistant*	Alfonso SCIROCCO (*) *Data Protection Officer* *Quality Management*
Vera POZZATO *Legal Officer*	Luis VELASCO *Technology Officer*

• Operations, Planning and Support

Andrea BEACH *Head of Sector*	Marta CORDOBA-HERNANDEZ *Administrative Assistant*
Christine HUC (*) *Administrative Assistant*	Kim DAUPHIN *Administrative Assistant*
Milan KUTRA *Administrative Assistant*	Kim Thien LÊ *Administrative Assistant*
Ewa THOMSON *Administrative Assistant*	

• Information and Communication

Nathalie VANDELLE (*) *Head of Sector*	Olivier ROSSIGNOL *Acting Head of Sector*
Agnieszka NYKA *Information and Communication Assistant*	Benoît PIRONET *Web Developer Contractor*

• Human Resources, Budget and Administration

Leonardo CERVERA NAVAS *Head of Unit*	Isabelle DELATTRE *Finance and Accounting Assistant*
Anne LEVÊCQUE *Human Resources Assistant* *GECO*	Vittorio MASTROJENI *Human Resources Officer*
Julia MALDONADO MOLERO *Contract Agent*	Daniela OTTAVI *Finance and Accounting Assistant*
Aida PASCU *Administration Assistant* *Assistant LSO*	Sylvie PICARD *Data Protection Officer* *COFO - ICC*
Anne-Françoise REYNDERS *Administration Assistant*	Maria SANCHEZ LOPEZ *Finance and Accounting Officer*

(*) Staff members who left the EDPS in the course of 2011

The European Data Protection Supervisor

Annual Report 2011

Luxembourg: Publications Office of the European Union

2012 — 117 pp. — 21 × 29.7 cm

ISBN 978-92-95073-28-9
doi:10.2804/35928

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-12-001-EN-C

The European guardian of personal data protection

www.edps.europa.eu

Publications Office

ISBN 978-92-95073-28-9