ISSN 1830-5474

Annual Report 2010

European Data Protection Supervisor

Annual Report

2010

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, 2011

ISBN 978-92-95073-19-7
doi:10.2804/20023

Printed in Luxembourg

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

Contents

6 ADMINISTRATION, BUDGET AND STAFF

7 EDPS' DATA PROTECTION OFFICER

8 MAIN OBJECTIVES IN 2011

USER GUIDE

Immediately following this guide, you will find a mission statement and a foreword presented by Peter Hustinx, European Data Protection Supervisor (EDPS), and Giovanni Buttarelli, Assistant Supervisor.

Chapter 1 — Highlights of 2010 presents the main features of the EDPS' work in 2010 and the results achieved in the various fields of activities.

Chapter 2 — Supervision describes the work done to monitor and ensure the EU institutions and bodies' compliance with their data protection obligations. This chapter presents an analysis of the main issues in prior checks, further work in the field of complaints, monitoring compliance and advice on administrative measures dealt with in 2010. It presents the thematic guidelines adopted by the EDPS in the fields of administrative enquiries and disciplinary proceedings and further work as concerns guidance on the video-surveillance. The chapter also presents the new EDPS policy on compliance and enforcement.

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: some new technological issues and new developments in policy and legislation.

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, information to the public and online information tools.

Chapter 6 — Administration, budget and staff details the main developments within the EDPS`s organisation, including budget issues, human resources matters and administrative agreements.

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

Chapter 8 — Main objectives in 2011 provides a brief look ahead and the main priorities for 2011.

The Report is completed by 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 the present Report is also available to provide a quick overview of key developments in the EDPS' activities in 2010.

Those who wish to get further details about the EDPS are encouraged to visit our website at http://www.edps.europa.eu. The website also provides for 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).

Along these lines, the EDPS aims to work strategically to:

- promote a 'data protection culture' within the institutions and bodies, thereby also contributing to improving 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 now replaced Article 286 of the EC Treaty.

This report covers 2010 as the sixth full year of activity of the EDPS as a new 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 second year of our common five-year mandate as the current members of this authority.

This year has once again been of major importance for the fundamental right to data protection. The Lisbon Treaty, ensuring a strong legal basis for comprehensive data protection in all areas of EU policy, has had an increasingly visible impact. The review process of the EU legal framework for data protection is shaping up and attracting increasing attention. Two key policy programmes - the Stockholm programme in the area of freedom, security and justice, and the Digital Agenda, as cornerstone for the Europe 2020 strategy - are demonstrating the relevance of data protection as a crucial element of legitimacy and effectiveness in both fields.

The EDPS has been strongly involved in these different contexts and is determined to pursue this course in the near future. At the same time, we have made sure that the role of an independent supervisory authority has been exercised in all main areas of activity and that its organisation is fully adequate. This has led to significant progress, both in supervision of EU institutions and bodies when they process personal data, and in consultation on new policies and legislative measures, as well as in close cooperation with other supervisory authorities to ensure greater consistency in data protection.

We therefore 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 the important challenges ahead.

Finally, we wish to express special thanks to our members of staff. The qualities that we enjoy in our staff are outstanding and contribute greatly to our effectiveness.

Peter Hustinx
European Data Protection Supervisor

Giovanni Buttarelli
Assistant Supervisor

1 HIGHLIGHTS OF 2010

1.1. Key features

Some recent developments have contributed to placing **fundamental rights and data protection** at the centre of the European agenda. The **Lisbon Treaty**, in force since 1 December 2009, has heightened the protection of fundamental rights in the European Union (EU) by giving the Charter of Fundamental Rights the same legal value as the Treaties and mandating the EU to accede to the **European Convention for the Protection of Human Rights and Fundamental Freedoms** (ECHR). With specific regard to data protection, Article 16 TFEU provides a general legal basis for the protection of individuals with regard to the processing of personal data by EU institutions and bodies, and by the Member States when carrying out activities which fall within the scope of EU law.

The importance of fundamental rights in general and data protection in particular is further highlighted in the **Stockholm Programme**, the current five-year policy programme in the area of freedom, security and justice. The Programme emphasised the need to ensure the respect of fundamental rights, freedom and integrity of persons, while guaranteeing security. Accordingly, respect for human rights and dignity and other rights set out in the Charter and the ECHR, particularly the right to privacy and data protection, are set as core values for Europe's action in this field. Significantly, the European Council invited the Commission to submit a proposal on the accession of the Union to the ECHR 'as a matter of urgency'.

These developments have also been backed up by other institutions. In connection with the Stockholm programme, the European Parliament significantly emphasised the role of fundamental rights for the future development of the area of freedom, security and justice [2]. The Commission itself recently adopted a Communication setting out a strategy for the effective implementation of the Charter in the new legal environment existing since the entry into force of the Lisbon Treaty.

The **review process of the data protection framework** initiated in 2009 and continued in 2010, is a decisive element of a Europe of fundamental rights. In November 2010, the Commission published a Communication laying down a comprehensive approach on personal data protection in the European Union. The Communication lays down the Commission's approach to modernising the EU legal framework for the protection of personal data in all areas of the Union's activities. The Communication intends to tackle the challenges brought by globalisation and new technologies so as to ensure a high level of data protection in the future. The EDPS is following the review process closely and has already contributed to it at various stages. This project will also continue to be one of our top priorities for 2011.

[2] European Parliament resolution of 25 November 2009 on the Communication from the Commission - An area of freedom, security and justice serving the citizen - Stockholm Programme, P7_TA(2009)0090.

In 2010, the Commission also invested considerable efforts in implementing the various initiatives linked with the Stockholm Programme. Several of these proposals are based on intensive data exchange between law enforcement or public security authorities of different countries and therefore, have a substantial impact on the privacy and data protection of individuals. When developing the **area of freedom, security and justice**, the European legislature constantly has to strike a balance between the security and free movement of citizens and the protection of their privacy and personal data. The implementation of the Stockholm Programme has been a key-feature of EDPS activities in 2010 and is likely to continue being so in the future.

Another important feature of the year concerns data protection issues relating to **new technologies**. Today's technology allows for the exchange and processing of data on an unprecedented scale. At the same time, data processing has become more subtle and less detectable. Social networks, cloud computing, road toll collecting, geo-location devices, behavioural advertising and similar new services all pose enormous challenges for data protection. The review of the data protection framework will have to deal with these challenges effectively in order to ensure high-level protection of personal data in a technology-driven world. New technologies are also at the centre of the initiatives included in the Commission's Digital Agenda for Europe. The EDPS will consider these initiatives and evaluate them whenever they raise issues for the data protection of individuals.

1.2. General overview of 2010

The main activities of the EDPS in 2010 have been based on the same overall strategy as before, but have continued to grow both in scale and in scope. The capacity of the EDPS to act both effectively and efficiently has also been improved.

The legal framework[3] within which the EDPS acts has provided 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[4] 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 developed in Chapters 2, 3 and 4 of this annual report, in which the main activities of the EDPS and the progress achieved in 2010 are presented. Some key elements will be summarised in this section.

The importance of information and communication concerning these activities fully justifies a separate emphasis on communication in Chapter 5. All these activities rely on effective management of financial, human and other resources, as will be discussed in Chapter 6.

Supervision

The 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 2010 the total number of DPOs reached 47. Regular interaction with them and their network is an important condition for effective supervision. A 'DPO quartet' composed of four DPOs (Council, European Parliament, European Commission and Translation Centre for the Bodies of the European Union) was set

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

(4) 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

up with the goal of coordinating the DPO network. The EDPS has collaborated closely with this quartet.

Prior checking of risky processing operations continued to be the main aspect of supervision during 2010. The EDPS adopted 55 prior-check opinions on standard administrative procedures, such as staff evaluation, recruitment, and promotions, but also on core business activities such as the Early Warning Response System for the exchange of information on communicable diseases. These opinions are published on the EDPS website and their implementation is followed up systematically.

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. Following the general monitoring exercise launched in spring 2009, the EDPS has continued to monitor the implementation of data protection rules and principles by the institutions and bodies involved. The next general monitoring exercise (Spring 2011) will begin in early 2011. Targeted monitoring exercises were also conducted where, as a result of his supervisory activities, the EDPS became concerned about the level of compliance at specific institutions or bodies. Some of these were correspondence–based, while others took the form of a visit to the body concerned. In 2010 the EDPS made two such visits. The EDPS also carried out an on-the-spot inspection at the Joint Research Centre of the Commission in Ispra to verify compliance on specific issues.

In 2010 the total number of **complaints** was 94; 25 of these were found to be admissible. Many inadmissible complaints involved issues at national level for which the EDPS is not competent. Most issues in admissible complaints involved alleged violations relating to access and rectification, misuse, excessive collection, and deletion of data. In 11 cases the EDPS concluded that data protection rules had been breached.

Further work was also done in **consultation on administrative measures** envisaged by EU institutions and bodies in relation to the processing of personal data. A variety of issues were raised, including international transfer of data, access to the identity of an informant, internal use of e-mails and e-monitoring.

The EDPS also adopted **guidelines** on administrative enquiries and disciplinary proceedings and video-surveillance.

In December 2010, the EDPS adopted a policy paper entitled 'Monitoring and Ensuring Compliance with Regulation (EC) 45/2001'. The paper sets out the framework within which the EDPS monitors, measures and ensures data protection compliance in the EU administration. It explains the nature of the various **enforcement powers** available to the EDPS and outlines the drivers and triggers for any formal action that he might take.

Consultation

In 2010, the Commission made significant progress towards a new, **modernised legal framework for data protection in Europe**. The public consultation launched in 2009 was concluded and supplemented with further targeted consultation with a number of key stakeholders. In November 2010, the Commission issued its Communication laying down a comprehensive approach on personal data protection in the European Union, identifying the main priorities and key objectives for the review of the current rules.

The EDPS gave special attention to the review process throughout 2010 and conveyed his messages in various ways. In particular, the EDPS held an *ad hoc* press conference immediately after the publication of the Communication to express his views publicly on the new legal framework. On this occasion, the EDPS emphasised the importance of the review, which he considered very timely and gave his perspective on the main points of the new framework.

The EDPS continued to implement his general **consultation policy** and issued a record number of 19 legislative opinions on different subjects. This policy also provides for a pro-active approach, involving a regular inventory of legislative proposals to be submitted for consultation and availability for informal comments in the preparatory stages of legislative proposals. Most EDPS opinions were followed up in discussions with the Parliament and the Council.

In 2010, the EDPS closely followed several initiatives directly connected with the implementation of the **Stockholm Programme**. Among others, the EDPS dealt with critical data protection issues relating to the EU Internal Security strategy, information management in the area of freedom, security and justice, the EU Counter-Terrorism Policy, Frontex and Eurodac Regulations. All in all, the developments concerning the Stockholm Programme have been

a dominant item in the EDPS agenda and will continue to be so in the coming years.

The **interface between privacy and technological developments** was also an area in which the EDPS intervened significantly. In May 2010, the Commission published its Communication on a Digital Agenda for Europe, with the objective to set EU priorities in the field of Internet and digital technologies. In March 2010, the EDPS adopted an opinion on 'Promoting trust in the information society by fostering data protection and privacy' as his input to this digital strategy. He also intervened in various ways on initiatives relating to the Internet and net neutrality, the review of the Data Retention Directive, the e-Waste Directive, the ENISA Regulation and e-justice.

The EDPS was also consulted on various initiatives in the field of **international cooperation on security and law enforcement**, such as the EU-US general agreement on data sharing for law enforcement purposes and the agreement on the exchange of financial data for the purposes of the Terrorist Finance Tracking Program (TFTP II). He also intervened with regard to the Anti-Counterfeiting Trade Agreement (ACTA) and agreements on the exchange of Passenger Name Records (PNRs).

The EDPS also intervened in other areas, such as taxation and customs (including administrative cooperation in the field of taxation and international customs cooperation), large-scale data exchanges taking place in the context of the Internal Market Information System, the use of security scanners at airports and various court cases about the relation between public access and data protection.

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 cooperated in good synergy on a range of subjects, especially on the implementation of the Data Protection Directive and on the interpretation of some of its key provisions. The EDPS contributed actively in different areas, such as the opinions on the concepts of 'controller' and 'processor', the principle of accountability and applicable law.

The EDPS also participates in the meetings and activities of the Working Party on Police and Justice, an advisory group dealing with former third pillar issues.

One of the most important cooperative tasks of the EDPS involves **Eurodac** where the responsibilities for supervision are shared with national data protection authorities. The Eurodac Supervision Coordination Group – composed of national data protection authorities and the EDPS – met three times in Brussels in March, October and December 2010. The Group started working on the preparation of the full security audit to be carried out by the data protection authorities, both at national and central (EU) level. A new coordinated inspection was launched at the end of 2010, the results of which are expected in 2011.

With regard to the supervision of the **Customs Information System (CIS)**, the EDPS convened two meetings of the CIS Supervision Coordination Group in 2010. The meetings gathered the representatives of national data protection authorities, as well as representatives of the Customs Joint Supervisory Authority and Data Protection Secretariat. At the December meeting, the Group adopted the Rules of Procedure which will govern its future work on CIS and discussed possible actions to be taken in the course of 2011-2012 to ensure comprehensive data protection supervision of the System.

The EDPS continued to cooperate closely with the authorities established to exercise **joint supervision on EU large-scale IT systems**.

Cooperation in **other international forums** continued to attract attention, especially the European and International Conferences of Data Protection and Privacy Commissioners held in Prague and Jerusalem, respectively.

In cooperation with the European University of Florence, the EDPS also organised a workshop on '**Data Protection in International organisations**'. The workshop addressed various challenges faced by international organisations trying to ensure a good level of data protection in sometimes difficult contexts and without a clear legal basis.

Some EDPS key figures in 2010:

➔ **55 prior-check opinions adopted,** notably on health data, staff evaluation, recruitment, time management, security investigations, telephone recording, performance tools

➔ **94 complaints received, 25 admissible.** Main types of violations alleged: violation of confidentiality of data, excessive collection of data or illegal use of data by the controller.

- **10 cases resolved** where the EDPS found no breach of data protection rules
- **11 declared cases of non-compliance** with data protection rules

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

➔ **1 on-the-spot inspection carried out**

➔ **2 guidelines published** on administrative enquiries and disciplinary proceedings and video-surveillance

➔ **19 legislative opinions issued** on initiatives relating to the area of freedom, security and justice, technological developments, international cooperation and data transfers, taxation and customs

➔ **7 sets of formal comments issued** on, among others, the revision of the Frontex Regulation, open Internet and net neutrality, Internal Market Information System, security scanners, international data exchange agreements

➔ **3 Eurodac Supervision Coordination Group meetings organised**, which resulted in the launch of new coordinated inspection, as well as preparations for a full security audit

➔ **12 new officials recruited**

1.3. Results in 2010

The following main objectives were set out in 2009. Most of these objectives have been fully or partially realised.

- **Support of DPO network**

The EDPS continued to give strong support to data protection officers and encouraged an exchange of expertise and best practices. Within the framework of their network, the DPOs developed a paper on 'Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) No 45/2001' which was finalised in October 2010. The EDPS sent a letter to all heads of institutions and agencies, endorsing the standards and underlining the importance of the DPO's role in achieving compliance with data protection rules as set out in the Regulation.

- **Role of prior checking**

The EDPS nearly completed prior checking of existing processing operations for most institutions and long-standing bodies and has put increasing emphasis on the follow-up of recommendations. This year, 137 cases were closed. Prior checking of common processing operations in agencies received special attention, as did addressing these cases through joint opinions.

- **Horizontal guidance**

To help ensure compliance in institutions and bodies and streamline prior checking procedures, the EDPS published guidance on administrative enquiries and disciplinary proceedings and video-surveillance.

- **Inspection policy**

In 2010, the EDPS continued the follow-up of previous inspections. Additionally, the EDPS carried out an inspection at the Commission's Joint Research Centre (JRC) in Ispra. In December 2010, the EDPS published a comprehensive policy on monitoring of compliance and enforcement of data protection rules in institutions and bodies.

- **Scope of consultation**

The EDPS issued a record number of 19 opinions and 7 sets of formal comments on proposals for new legislation, on the basis of a systematic inventory of relevant subjects and priorities and has

ensured the adequate follow-up thereof. All opinions and comments as well as the inventory, are available on the website. Special attention was given to the Action plan for the implementation of the Stockholm Programme.

- **Review of legal framework**

On a number of occasions, using different tools, the EDPS pushed for an ambitious approach in developing a modern, comprehensive framework for data protection, covering all areas of EU policy and ensuring effective protection in practice, which can deliver legal certainty for many years. The views of the EDPS are now also laid down in an opinion issued in January 2011.

- **Digital Agenda**

The EDPS focused his activities in the area of consultations on the main challenges for the effective protection of personal data. This means ensuring a proper balance between the need for security and data protection, dealing with technological developments and addressing the effects of worldwide data flows. Special attention was given to the Commission's Digital Agenda in an opinion adopted in March 2010, further elaborating the principle of 'Privacy by Design'.

- **Information activities**

The EDPS continued to improve the quality and effectiveness of communication actions and information tools. A major development in that respect was the introduction of German as a third language, in addition to English and French, in press and communication activities.

- **Internal organisation**

The Secretariat of the EDPS was reorganised in order to clarify responsibilities and ensure a more effective and efficient execution of his different roles and tasks. In the new organisational structure, the Director ensures the implementation of policies and horizontal coordination of activities taking place in five different sectors. The new Organisation Chart is available on the website.

- **Resource management**

In the course of 2010, there was a substantial increase (one third) in the number of EDPS staff. In conjunction with the internal reorganisation, new efforts in planning, internal procedures and budget implementation were required. Special attention was given to the need for additional office space and the development of a case management system.

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 Lisbon Treaty marks a change in the legal framework for data protection in the European Administration with the introduction of Article 16 of the Treaty on the Functioning of the European Union, which replaces Article 286 of the EC Treaty. The abolition of the pillar structure has resulted in the situation that the EDPS' supervisory tasks now in principle cover all EU institutions and bodies – also in areas wholly outside the scope of what used to be 'Community law'([5]) – except to the extent that other EU acts specifically provide otherwise. The precise implications of these changes for the supervision activities of the EDPS are still being examined and may require further clarification.

The prior checking of processing operations has continued to be an important aspect of supervision during 2010 (see Section 2.3), with special emphasis on the follow-up of recommendations made in his opinions. The EDPS has also developed other forms of supervision, such as the handling of complaints, inspections, advice on administrative measures and the drafting of thematic guidelines. The supervision of Eurodac is a specific activity of the EDPS requiring close cooperation with national data protection authorities (see Section 4.2).

The EDPS also adopted a policy on compliance and enforcement signalling a change of gear in enforcement of the Regulation.

2.2. Data protection officers

An interesting feature in the data protection landscape of the European Union institutions is the 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 also appointed data protection coordinators in order to coordinate all aspects of data protection within a particular directorate or unit.

In 2010, two new DPOs were appointed in new agencies or joint undertakings, bringing the total number of DPOs to 47.

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

([5]) See Article 3(1) of Regulation (EC) No 45/2001, which is now less relevant than before 1 December 2009.

has proved to be productive in terms of collaboration and continued throughout 2010.

A 'DPO quartet' composed of four DPOs (the Council, the European Parliament, the European Commission and the Translation Centre for the Bodies of the European Union) was set up with the goal of coordinating the DPO network. The EDPS has collaborated closely with this quartet.

The EDPS attended the DPO meetings held in March 2010 at the European Investment Bank in Luxemburg and the European Medicines Agency in London in October 2010 and took the opportunity to update the DPOs on EDPS work, give an overview of recent developments in EU data protection and to discuss issues of common interest.

More specifically, the EDPS used this forum to explain and discuss the procedure for prior checks; report on progress in prior checking notifications; update the DPOs on the discussions with inter-institutional committees; explain the new EDPS structure and to present EDPS thematic guidelines. The EDPS also informed the DPOs about the adoption of the compliance and enforcement policy. The forum is also used to share initiatives for European Data Protection Day (on 28 January).

Within the framework of their network, the DPOs developed a paper on 'Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001' which was finalised at the meeting of the DPO network on 14 October 2010. The EDPS sent a letter to all heads of institutions and agencies endorsing the standards and underlining the importance of the role of the DPO in the achievement of compliance with data protection rules as set out in the Regulation. The EDPS intends to build on this paper, where appropriate, in his supervisory role with regard to institutions and bodies.

2.3. Prior checks

2.3.1. Legal base

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

Article 27(2) of the Regulation contains a non-exhaustive list of processing operations that are likely to present such risks. The criteria developed in previous years[6] continued to be applied in the interpretation of this provision, both when

[6] See Annual Report 2005, section 2.3.1.

Data protection officers during their meeting in Brussels (March 2010).

deciding that a notification from a DPO was not subject to prior checking and when advising on a consultation as to the need for prior checking (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).

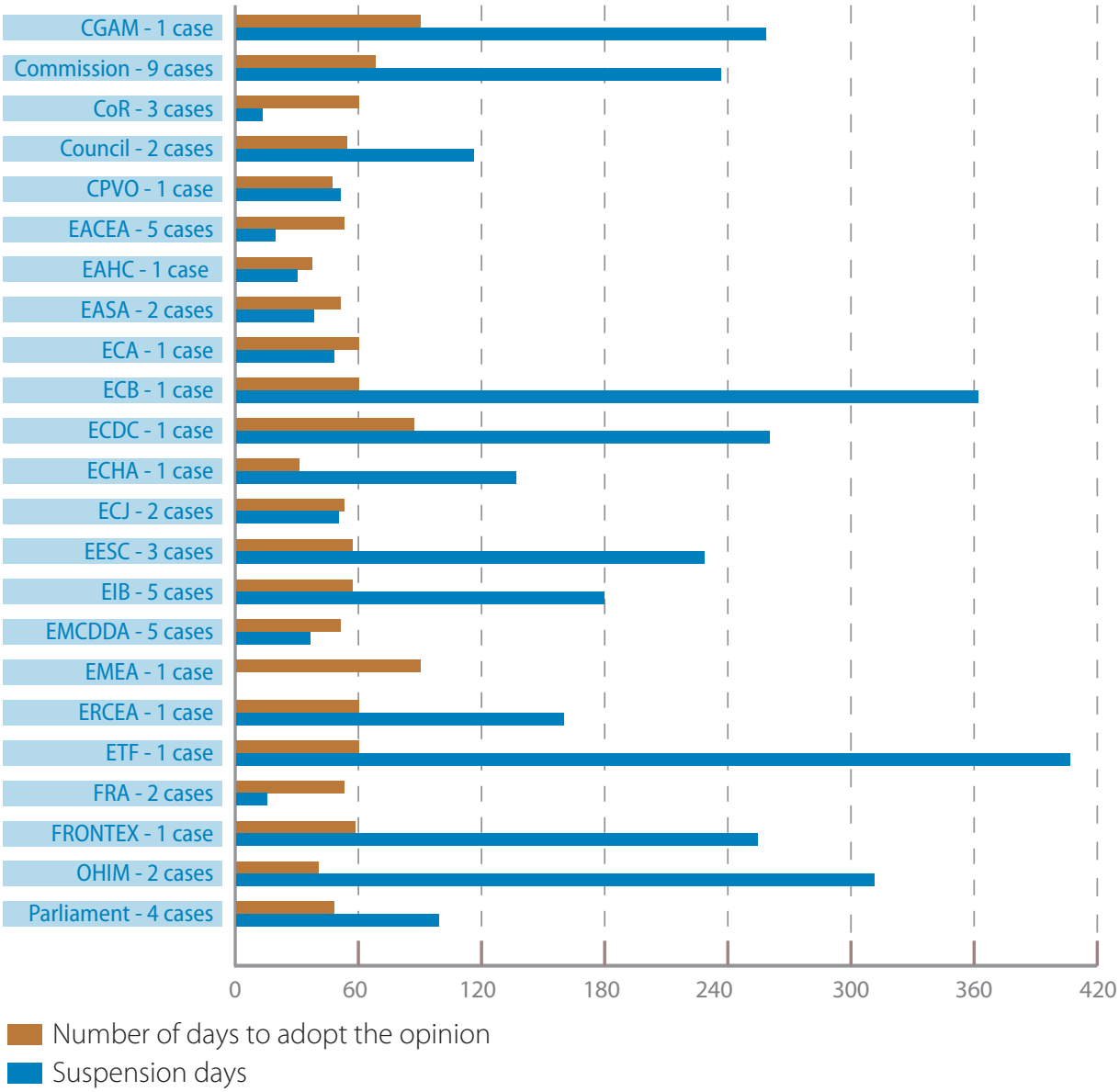
Prior checks involve operations not yet in progress and also processing that started before 17 January 2004 (the appointment date of the first EDPS and Assistant EDPS) or before the Regulation came into force (*ex-post* prior checks). In such situations, an Article 27 check cannot be 'prior' in the strict sense of the word, but must be dealt with on an *ex-post* basis.

Period, suspension and extension

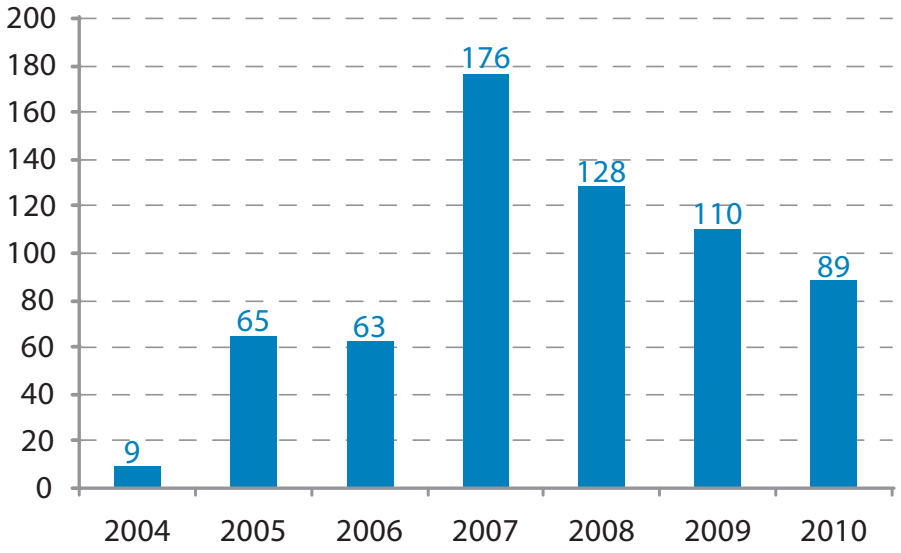
The EDPS must deliver his opinion within two months of receiving the notification([7]). Should the EDPS make a request for further information, the period of two months is usually suspended until

([7]) For ex-post cases received before 1 September 2010, the month of August has neither been calculated for institutions and bodies, nor for the EDPS.

Average deadlines per institution/agency



Notifications to the EDPS



the EDPS has obtained this information. This period of suspension includes the time given to the DPO for comments and further information if needed, 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.

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

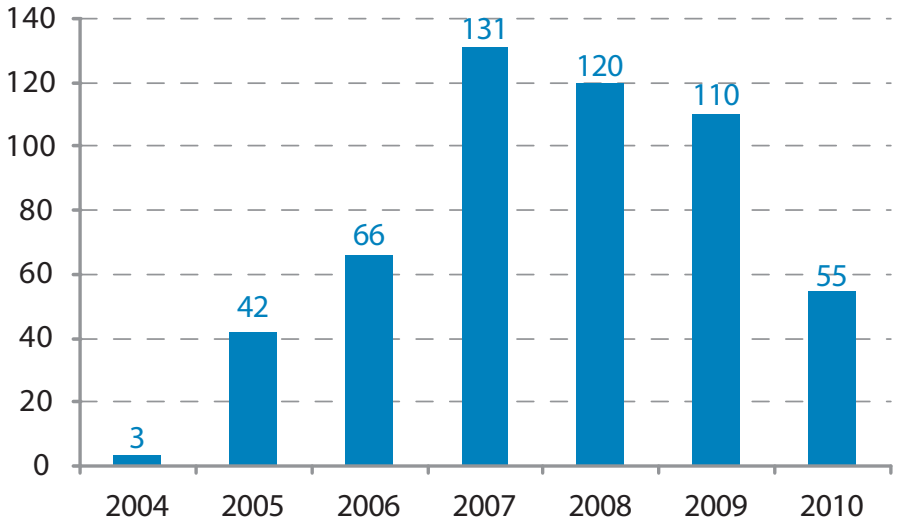
Register

In 2010, the EDPS received 89 notifications for prior checking. This figure shows a slight decrease in comparison to 2009 as the EDPS reaches the end of the backlog of *ex-post* prior checks.

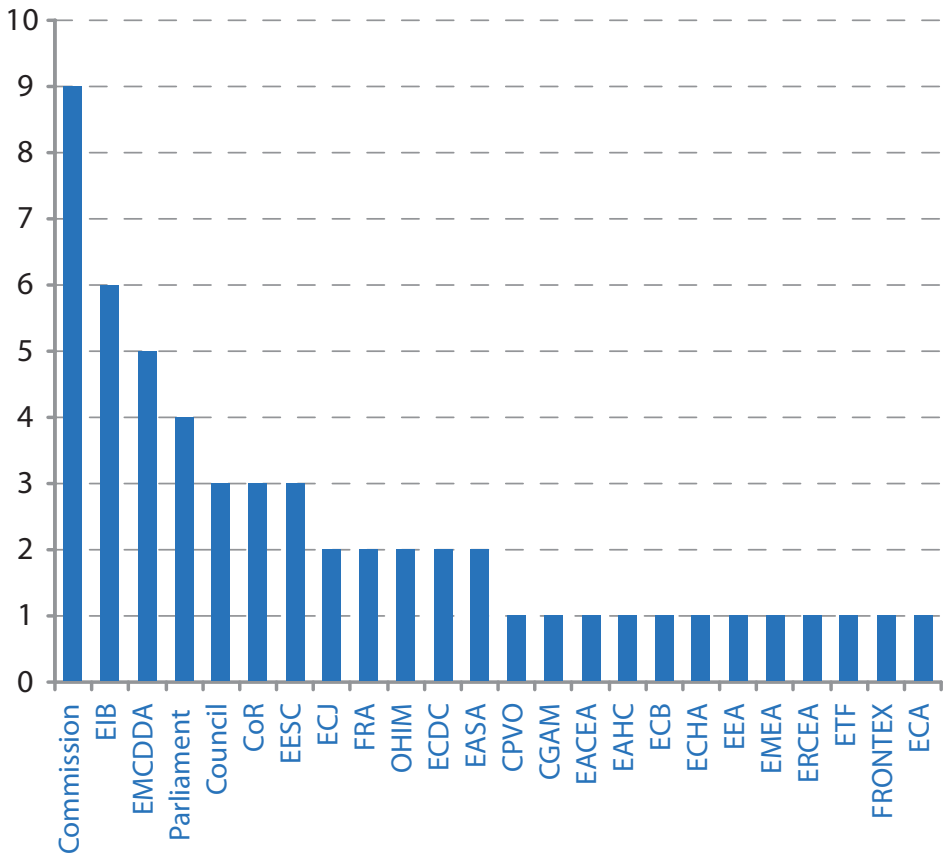
Opinions

The final position of the EDPS takes the form of an opinion, notifying the controller of the processing operation and the DPO of the institution or body (Article 27(4)). In 2010, the EDPS issued **55 prior**

EDPS prior-check opinions per year



EDPS prior-check opinions per institution in 2010



checking opinions (see above chart 'EDPS prior-check opinions per year') and **8 on 'non-prior checks'** (see Section 2.3.5). Although this represents a decrease compared to previous years, it is worth noting that, following the guidelines on video-surveillance and recruitment, the EDPS has dealt with a significant number of cases through joint opinions, thereby dealing with these issues in a more efficient manner.

A **major portion of these opinions** were for the **larger institutions,** with nine prior checking opinions (and three non-prior checks) relating to processing operations at the European Commission, four at the European Parliament and three at the Council (see chart 'EDPS opinions per institutions'). The agencies have also continued notifying core business activities and standard administrative procedures according to the relevant procedures drawn up by the EDPS (see Section 2.3.2).

Opinions contain a description of 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 to the controller so as to comply with the Regulation. In the conclusion, 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.

Once the EDPS has delivered his opinion, it is made public. All opinions are available on the website of the EDPS, together 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 agencies

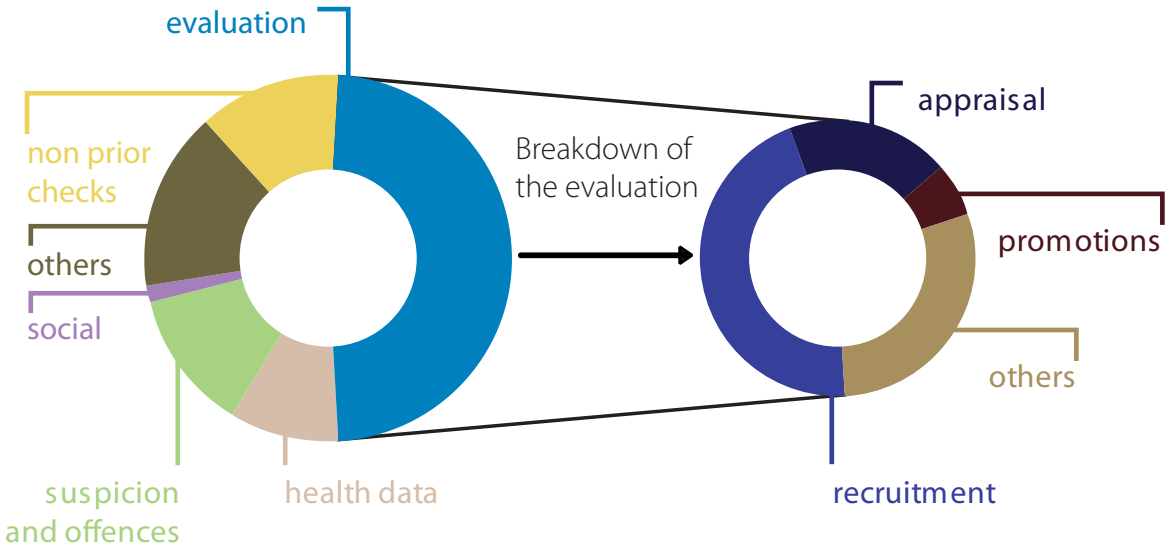
In October 2008, the EDPS launched a new procedure for *ex-post* prior checks in the EU agencies. Since standard procedures are the same in most EU agencies and are based on Commission

decisions, the idea is to gather notifications on a similar theme and to adopt either a collective opinion (for various agencies) or a 'mini prior check' addressing only the specific needs of an agency. To help the agencies complete their notifications, the EDPS submits a summary of the main points and conclusions on the relevant theme based on previous prior-checking opinions in the form of thematic guidelines (see Section 2.7 Thematic Guidelines).

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**. At the time of writing, the EDPS has sent his draft horizontal opinion to the 19 agencies involved for comment and hopes to adopt this in early 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. The EDPS is presently receiving notifications from agencies in this field and intends to adopt a joint opinion in the first six months of 2011.

2.3.3. Main issues in prior checks

Opinions 2010 per category



2.3.3.1. Early Warning Response System - European Commission

The Early Warning Response System (EWRS) is a communication tool used by the Commission, the European Centre for Disease Prevention and Control (ECDC) and EU Member States, to exchange information relating on the prevention of communicable diseases (such as tuberculosis, measles, SARS, H1N1 and others) in order to facilitate cross-border action. One feature of the EWRS is '**contact tracing**' - a procedure used to identify and reach persons who may have come into contact with an infected person. Once contacts are traced, they may be diagnosed and receive care. Contact tracing also serves general public health interests by reducing or preventing the further spread of the disease.

In his opinion (Case 2009-0137), the EDPS focused on the need to **clearly establish the roles, tasks and responsibilities** of the parties involved in operating and using the system, in particular, the roles of the Commission and the ECDC. Controllers and processors must be clearly designated in a way which corresponds to their effective roles, as well as the legal status of the organisations involved.

The responsibilities of the parties involved and how data subjects can exercise their rights must be clearly specified. In the short term, the EWRS was advised to adopt a set of data protection guidelines. The Commission was also encouraged to revise the legal framework to ensure a more secure legal basis and clear allocation of responsibilities.

The EWRS is a communication tool for the exchange of information on communicable diseases.

In addition, the EDPS emphasised the need for implementing the principle of '**Privacy by Design'**, and integrating data protection into the training provided to users. A clear mechanism should be provided for data subjects to exercise their **right of access**. Finally, to ensure consistency and transparency, the operator of the EWRS should provide comprehensive and user-friendly information to data subjects on its website. This should be complemented by notices provided by Member State contact points in accordance with national data protection laws.

2.3.3.2. European Surveillance System ('TESSy') - European Centre for Disease Prevention and Control

On 3 September 2010, the EDPS issued a prior checking opinion (Case 2009-0474) on the data protection aspects of TESSy. TESSy is a communication tool of the European Centre for Disease Prevention and Control designed to ensure a rapid and effective exchange of epidemiological surveillance data among EU Member States.

The opinion explains that **statistical data** continue to be considered as 'personal data', and therefore subject to the Regulation, so long as the individuals can be at least indirectly identified. The fact that certain 'anonymisation techniques have been used' does not necessarily mean that the data are considered as 'anonymised' within the meaning of Recital 8 of the Regulation and thus, cease to be considered as 'personal data'.

The EDPS reiterated many of the recommendations made in his opinion on the EWRS (see above) and added that a specific security policy should be adopted as soon as possible to help ensure the security of TESSy.

2.3.3.3. Joint Sickness Insurance Scheme

The Joint Sickness Insurance Management Committee (JSIMC) is responsible for the operation of the Joint Sickness Insurance Scheme. The JSIMC is comprised of staff representatives appointed by the Staff Committees of each institution and representatives of the administrations. It deals with all amendments to the rules, complaints by members and issues opinions, recommendations and proposals concerning the operation of the Scheme.

The EDPS met the JSIMC in November 2008 in order to discuss data protection issues in relation to the files managed by the JSIMC. Since the affiliated members' complaints often contain sensitive data, it was decided that the Committee would send a notification to the EDPS.

This notification led to an opinion (Case 2009-0070), issued on 18 January 2010, in which the EDPS made recommendations notably on the **transmission of personal data** to the JSIMC; the **retention period** on CIRCA (a web-based application for workgroups using shared data) and the adoption of an **appropriate security policy** within six months after adoption of the opinion.

2.3.3.4. Safety inspections - European Commission (DG Joint Research Centre, Ispra)

On 6 September 2010 (Case 2009-0682), the EDPS issued a prior-check opinion on safety inspections at the European Commission's Joint Research Centre in Ispra. It involved the data processing operations carried out for the purpose of maintaining and improving the applicable safety standards.

The EDPS acknowledged that the 'Procedura in caso d'infortunio' involves the processing of health related data by several parties with the aim of preventing and minimising the consequences of similar safety incidents at the Ispra site.

The EDPS issued recommendations in order to **guarantee the respect of the 'purpose limitation' principle in case of transfers of data**, as well as **compliance with the data quality principles** applicable to the storage and further processing of personal data processed in this context. A corresponding revision of the existing privacy statement was also suggested.

2.3.3.5. BELBIN Self perception inventory - European Administrative School

The purpose of the processing is to allow participants in the European Administrative School (EAS) training courses to obtain feedback in the form of a report on their preferred role in a team. The data is not to be used for any form of appraisal on the individual concerned. In his opinion of 15 March 2010 (Case 2009-0377), the EDPS concentrated on two aspects:

- **the relationship between the controller, the processor and the sub-contractor**: even if the EAS has no access to the data processed by the sub-contractor, the sub-contractor must act according to the instructions given by the EAS to the contractor. The EAS is the data controller of this processing activity because it determines the purposes and the means of use (the web-based tool). The three contractors responsible for providing the training courses and the subcontractor responsible for the web-based tool are all considered processors of personal data acting on EAS' behalf. The sub-contractor is not authorised to carry out any further processing activity beyond what is determined by the EAS and specified in the contract between the subcontractor and the contractor in accordance with the contract between the EAS and the contractor;

- **the anonymous nature of the data**: the report given to the participants cannot be considered 'anonymous' because the sub-contractor is able to link the answers to data subjects as the participants usually use an e-mail address which indicates their name and forename.

The EDPS made recommendations on these two aspects, in particular that the contract should include clauses on all mandatory items, notably **confidentiality and security relating to the processing** between the contractor and the sub-contractor.

2.3.3.6. E-monitoring - Court of Auditors

A procedure to **access private drives and e-mails** has been developed by the **Court of Auditors (**ECA) in order to deal with various situations (e.g. staff who pass away, leave the institution or are absent) where the information contained therein is necessary for the functioning of the institution. The proposed procedure requires the person requesting the information to fill in a standard form. The request should contain a detailed description of the reason(s) justifying the access, the file name(s) or e-mail account and/or the subject of the information. The form should be sent to the Information Security Officer or, in his absence, to the Physical Security Officer.

A procedure to access private drive and emails was developed at the Court of Auditors.

Originally the request was sent to the EDPS for consultation, as this procedure **potentially involves access to confidential data** and the EDPS indeed considered that the processing operation presented specific risks requiring a notification for prior-checking.

In his opinion of 10 January 2010 (Case 2009-0620), the EDPS recommended that the ECA adopt a **specific legal basis** for the use and storage of private e-mail and establish **clear user guidance** on the use of network resources and e-mails.

2.3.3.7. Salary deductions in the event of a strike - European Central Bank

According to Article 1.4 of the Staff Rules of the European Central Bank (ECB), staff members have the right to strike. Article 1.4.5 provides that 'Unless the Executive Board decides otherwise, the total period of the strike shall be deducted from the salary related payments of the member of staff taking part in the strike'. Furthermore, 'no disciplinary action may be taken against any member of staff participating in a strike unless the member of staff has been nominated to provide the minimum services described above and fails to do so in order to take part in the strike' (Article 1.4.7).

To the extent that participation in a strike automatically entails a deduction from salary and other allowances, the processing of personal data related to that deduction is subject to prior checking by the EDPS, as it entails processing which excludes individuals from a right, benefit or contract.

On 28 September 2010, the EDPS issued a prior checking opinion (Case 2009-0514) regarding such a processing operation, making recommendations on the **conservation periods** of any documentation stored in the ECB's electronic document and record management system and the **information** to be provided to the data subjects.

2.3.3.8. Fraud investigations - European Investment Bank

The European Investment Bank (EIB)'s Fraud Investigation Division (IG/IN) investigates allegations of prohibited practices in accordance with the EIB Anti Fraud procedures. In order to conduct investigations, the IG/IN has full access to all relevant information, documents and data on personnel, including electronic data within the EIB, although no interception of communications or conversations is permitted. The Head of IG/IN will determine whether a complaint or allegation has been substantiated and will refer the case to the relevant authorities within and/or outside the EIB for appropriate action. If, after reasonable investigation, IG/IN determines that a complaint or allegation has not been substantiated, it shall document the findings in a note on the file and close the case.

The EDPS issued a prior check opinion (Case 2009-0459) on the data processing operations related to such fraud investigations, and recommended that the EIB examines the **legal basis** of these investigations; adopts a **formal protocol for conducting computer forensic** investigations; harmonise the conservation periods and provide information to data subjects.

2.3.3.9. Empirical analysis of correlations between work system variables and decision-making - Office for Harmonisation in the Internal Market

This prior checking (Case 2010-0468) covered the data protection aspects of an exercise undertaken by the Office for Harmonization in the Internal Market (OHIM) entitled 'Empirical analysis of correlations between work system variables and decision-making'. The aim of the analysis was to help identify comparable job profiles and develop best practices in human resources management for

The EIB Fraud Investigation Division investigates allegations of prohibited practices.

these profiles. In addition to bringing practical benefits to the OHIM, the project also had additional scientific purposes, as the analyst carrying out the research planned to publish the findings in a PhD thesis (after careful editing to protect the privacy of the participants in the exercise). The EDPS provided a number of recommendations, notably on data retention, transfers to third parties and information to data subjects.

The EDPS recommended that all personal data from the OHIM servers should be deleted at the end of the conservation period (2011). The EDPS also advised the analyst to take account of applicable national law regarding any microdata retained for potential future research purposes or transferred to third parties, to ensure compliance with necessity, purpose and confidentiality obligations.

2.3.3.10. The Central exclusion database - European Commission

In order to protect the financial interests of the institutions and on the basis of the Financial Regulation, the European Commission processes data which are contained in a central exclusion database. Such data may only be used for the purposes of excluding entities which represent a threat to European financial interests from any procurement or grant procedures funded with the EU funds or the European Development Fund.

The EDPS conducted his analysis (Case 2009-0681) in full cooperation with the institution from an early stage.

The EDPS concluded that there was no reason to believe that there was a breach of the provisions of the Data Protection Regulation. He did however make some recommendations regarding the prior information of candidates, tenderers and grant applicants to be provided in the call for proposals and call for tenders.

2.3.3.11. Joint return operations - FRONTEX

On 26 April 2010, the EDPS adopted an opinion (Case 2009-0281) on the processing of personal data by FRONTEX regarding the 'collection of names and certain other relevant data on returnees for joint return operations (JRO)'. The purpose of the processing is the preparation and realisation of JROs assisted by FRONTEX in order to provide airlines with

a passenger list and to know, among others, the number and identification of returnees, the risks linked to the returnees and for the security of the JRO and the state of health of the returnees to secure appropriate medical assistance during the JRO.

FRONTEX informed the EDPS that personal data had not been processed for operational activities so far, but that this would be necessary in the near future to 1) better fulfil and further develop the Agency's task in the context of the JRO 2) assist an organising Member State or Schengen associated country in compiling passengers lists and updating them 3) have a constant overview of which participating Member State or Schengen associated country have (or have not) provided the required data to the organising State 4) increase the effectiveness and efficiency of FRONTEX assistance in organising JRO.

The EDPS paid particular attention to the legal basis of the processing. The EDPS recognised that some processing of personal data may be necessary for a proper execution of the Agency's task in the context of the JRO and for which the Agency should be seen as a controller. However, due to the sensitivity of the data and the activities concerned with regard to a vulnerable population, the EDPS considered that Article 9 of the FRONTEX Regulation (Return cooperation) and Article 5(a) of the Data Protection Regulation can only serve as a provisional legal basis for the processing activity, which should be the subject of a careful review of the need for a more specific legal basis.

The EDPS also requested that FRONTEX implements the necessary **procedures to guarantee the rights of the data subjects** and implements the **obligation to inform** before the processing activity takes place.

2.3.4. Consultations on the need for prior checking

The mere possibility of the presence of **sensitive data** does not automatically make it a case for 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. During 2010, the EDPS received six such consultations from DPOs.

Among the issues considered by the EDPS were the selection procedures for senior staff; attendance lists of members of associations participating in events at an institution; processing activities of a Staff Committee and a staff training policy.

2.3.5. Notifications not subject to prior checking or withdrawn

Following careful analysis, eight cases were not found to be subject to prior checking in 2010. In these situations (also referred to as 'non-prior checks'), the EDPS may still make recommendations. Furthermore, three notifications were withdrawn and one was replaced.

In a case related to training (Case 2010-0638), further information received from the European Food Safety Authority (EFSA) in the context of the notification, clarified that the data collected mainly concerned statistics and was intended only for quality assurance purposes of the EFSA Training Policy. Although trainer evaluation data may be included, the report produced was not intended to evaluate individual trainers. Based on this information, the EDPS concluded that this notification was not subject to prior-checking.

2.3.6. Follow-up of prior-checking opinions

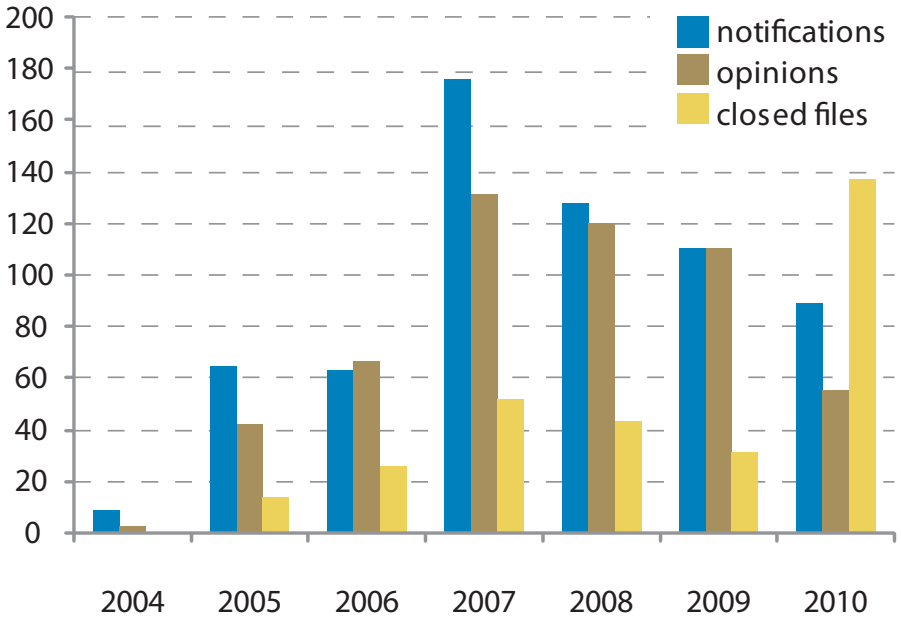
*An EDPS prior check opinion will usually conclude by stating that the processing operation does not violate the Regulation providing certain **recommendations** are implemented. Recommendations are also issued when a case is analysed to decide on the need for prior checking and some critical aspects 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 Regulation (EC) No 45/2001.*

Institutions and bodies have willingly followed the recommendations of the EDPS and up to now, 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 recently published 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. That is they must be responsible for implementing them and be able to demonstrate this to the EDPS. Any institution or body failing to act on the recommendations, will thus risk formal enforcement action.

Comparative situation



2.3.7. Conclusions

The 55 opinions given by the EDPS have provided valuable insight into the processing operations of the European administrations and have enabled the EDPS to build on its expertise and provide generic guidance in certain areas, such as in common administrative procedures. This is evident in the processing related to administrative inquiries and disciplinary proceedings (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.

As most institutions reached the end of the notification of their existing processing operations in standard administrative procedures, the EDPS received many notifications during 2010 on core business processes specific to certain institutions or agencies.

The EDPS reached an important milestone in the follow-up of EDPS prior checking opinions, as 137 cases were closed in 2010. 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. Only EU staff can complain about an 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 a complaint to the EDPS (Article 90b).

Any person can complain to the EDPS about the processing of personal data by the EU administration.

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 a 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.*

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 staff member of the European Commission questioned the content of his evaluation report prepared by the hierarchy. He requested the EDPS to order the Commission to rectify the report, as it contains his personal data. The EDPS did not follow the reasoning of the complainant. In fact, even if the evaluation data are personal data, there are by definition subjective assessments which cannot by automatically rectified on the basis of data protection rules. A specific procedure designed to challenge the content of evaluation reports should be followed to question the inclusion of data.

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 the 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. 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.

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 may advise the complainant to address the matter to another competent authority (e.g. the Court of Justice, the Ombudsman, national data protection authorities, etc.).

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 which 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 person questioned the EDPS as to whether she could get access to the personal data of other candidates in a recruitment procedure or whether this could be denied to her on data protection grounds. The EDPS did not take a position as the question was still hypothetical given the fact that the EU body in question had not yet refused access to the information requested and had therefore not yet used data protection as a reason for refusal.

The 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 contacting it.

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, in principle, admissible. 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. Among other things, it stipulates that a complaint that has already been examined should not be reopened by another institution unless significant new evidence is submitted.

As 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**. This inquiry can include a request for information to the institution concerned, a review of relevant documents, a meeting with the controller, an on-the-spot inspection, etc. The EDPS has the power 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 his decision, the EDPS expresses his opinion on any breach of the data protection rules by the institution concerned. The **powers of the EDPS** are broad, ranging from simply giving advice to data subjects through 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.

On two occasions in 2009, the complainants challenged the decisions of the EDPS before the General Court (cases T-164/09 and T-193/09). As to the first case, the Court decided that there was no longer any need to rule on the EDPS action because the action had become devoid of purpose. As to the second case, the application for legal aid submitted by the plaintiff was rejected by the Court. 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 difficult 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.

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 by the EDPS on the 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 which 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 2010

2.4.4.1. Number of complaints

The complexity of complaints received by the EDPS increased in 2010, even though the number decreased. ***In 2010, the EDPS received 94 complaints*** *(a decrease of 15% compared to 2009). Of these,* ***69 complaints were inadmissible****, the majority relating to processing at national level as opposed to processing by an EU institution or body.*

The remaining 25 complaints required more in-depth inquiries (a decrease of 41% compared to 2009). In addition, 18 admissible complaints, submitted in previous years (16 in 2009 and two in 2008), were still in the inquiry or review phase during 2010.

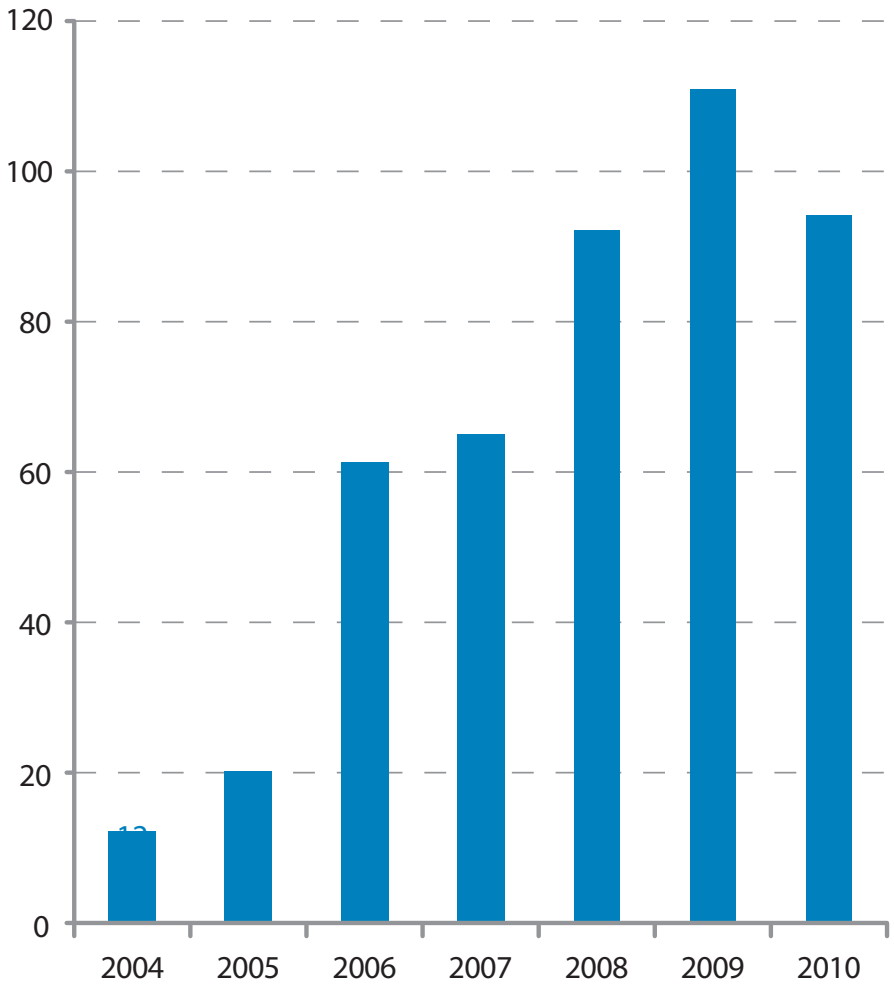
2.4.4.2. Nature of complainants

Of the 94 complaints received, 17 complaints (18%) were submitted by members of staff of EU institutions or bodies, including former staff members and candidates for employment. For the remaining 77 complaints, the complainant did not appear to have an employment relationship with the EU administration.

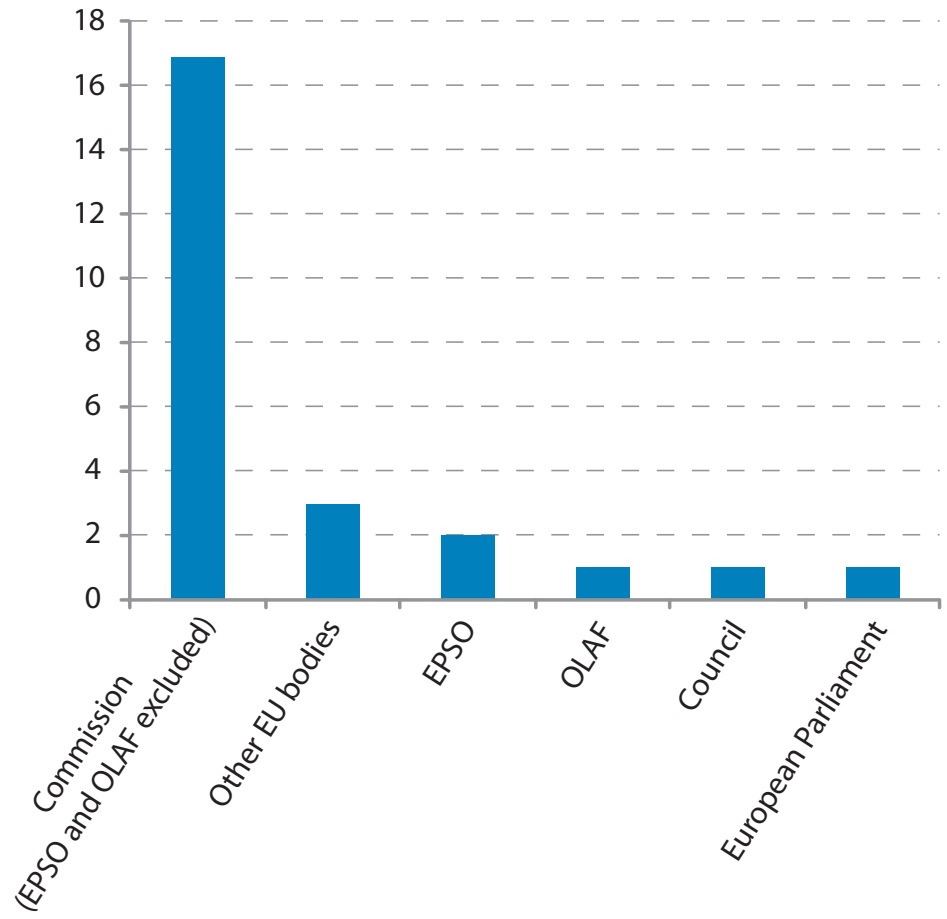
2.4.4.3. Institutions concerned by complaints

Of the admissible complaints submitted in 2010, the majority (80%) were directed against the **European Commission, including OLAF and EPSO**. This is to be expected since the Commission conducts 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.

Number of complaints received (evolution 2004-2010)



EU institutions and bodies concerned



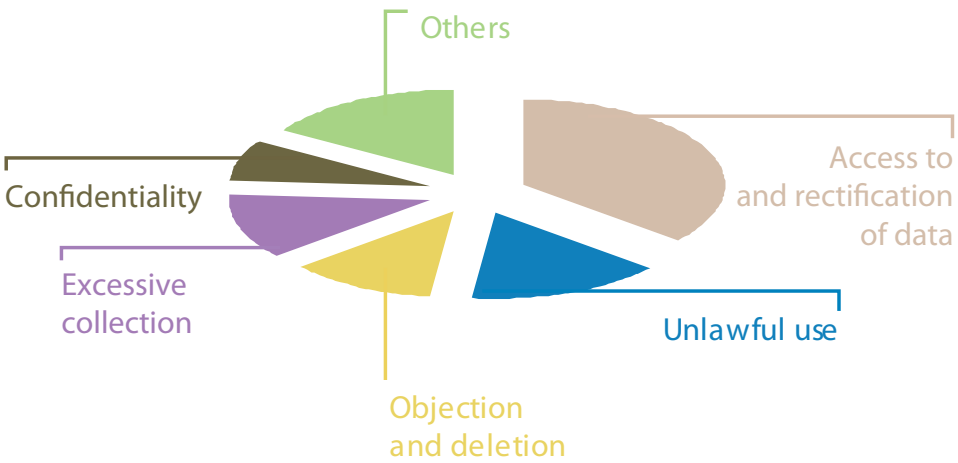
2.4.4.4. Language of complaints

The majority of complaints were submitted in English (44%) or German (33%), French (15%) being less commonly used. 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 2010 mainly relate to:

Types of violations alleged



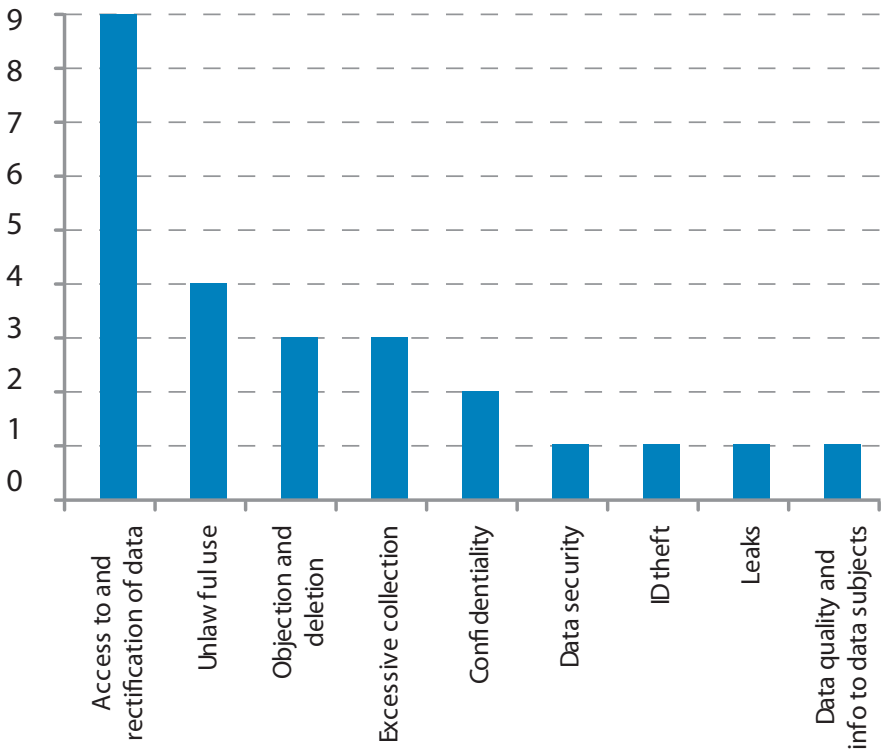
- A breach of data subjects' rights, such as access to and rectification of data (36%) or objection and deletion (12%);
- Unlawful use (16%), excessive collection of personal data (12%), violation of confidentiality (8%).

Other violations less frequently alleged relate to data security (4%), ID thefts (4%), leaks (4%), data quality and information to data subjects (4%).

2.4.4.6. Results of EDPS enquiries

In 10 cases resolved during 2010, the EDPS found there was no breach of data protection rules.

Result of EDPS enquiries



The EDPS received a complaint relating to access to one's own medical file held by an institution's medical service. The EDPS confirmed that under the data protection rules, access to personal data does not oblige the controller to send the original medical file, but that it implied in practice being able to have a look at it (in person or in certain cases indirectly via a doctor) and/or take copies of it. With regard to the right to rectification of inaccurate or incomplete data, the EDPS underlined that the obligation to rectify data in the context of medical data is related only to factual data and not to health-related assessments. The controller is therefore not obliged under data protection rules to modify the conclusion of a specific medical report. In such a context, the right to rectify the data could result in the possibility to include another report from another medical professional containing a different assessment. The EDPS therefore concluded in this case that there was no breach to data protection rules.

Conversely, in 11 cases, non-compliance with data protection rules was found to have occurred and recommendations were addressed to the data controller.

A complaint was received about the publication of highly sensitive personal data in the Official Journal of the European Union and in the minutes of a European Parliament session. Following an inquiry into the matter, the EDPS concluded that the opinion of the Member of Parliament could have been expressed and the political message of the Written declaration could have been transmitted effectively without revealing the identities of the persons concerned. The EDPS requested the deletion of the names of the persons invoked by the Member in the Written declaration and in any other medium. He also requested that a formal and effective procedure be established in order to ensure that definitive versions of documents published in the Official Journal and on the internet site of the Parliament take into account modifications introduced by the services in charge of the preparation of documents.

A complaint was received relating to the communication of personnel numbers of the members of staff of an agency to all users via the agency's internal email addresses. The purpose of the particular processing was to invite all members of staff for an appointment with the agency's Security section to have their photograph taken. The EDPS considered that, for this purpose it was fully sufficient to send a list containing only last name and first name of all the persons concerned. The personnel number on this list was irrelevant and excessive in relation to the said purpose and thus in violation of Article 4 of the Regulation. The EDPS invited the agency to formally instruct staff dealing with personal data to be selective and exercise particular care when sending massive internal or external mailings containing personal data so as to ensure that only data which are necessary for the purpose of the message are included.

A staff member complained against covert video-surveillance in his institution. In particular, he questioned the lawfulness of the use of a video-camera which recorded him, without his knowledge, when he entered his supervisor's office in his absence. The EDPS concluded that the institution had not demonstrated the existence of a legal basis which would explicitly allow the possibility of such highly intrusive operations and provide for specific conditions and safeguards. Without such a transparent legal basis and a structured approach, the proportionality of covert video-surveillance was doubtful. The EDPS, therefore, called on the institution to re-examine whether it wished to avail itself of covert surveillance in the future and if so, to submit its plans to the EDPS for prior checking.

2.4.5. Further work in the field of complaints

The EDPS intends to facilitate the process of submitting complaints and speed up the processing of complaints by the EDPS services by providing an **on-line complaint submission form** on the EDPS website (see Section 5.6.1). A provisional version of such a form has been available on the EDPS website since early 2010. The final version will be more interactive. The EDPS expects that the generalisation of the use of this application will help complainants to assess the admissibility of their complaint and thereby submit only relevant matters to the EDPS. In addition, the EDPS hopes to obtain more complete and relevant information to handle complaints more efficiently and reduce the number of manifestly inadmissible complaints

The EDPS also intends to review the manual of internal procedures for complaints handling, adopted in 2009. The modified procedures would integrate the new organisational structure of the EDPS and clarify the internal workflow of complaint cases.

2.5. Monitoring compliance

*The EDPS is responsible for monitoring and **ensuring the application of Regulation (EC) No 45/2001**. Monitoring has mainly been performed by a **reporting exercise** referred to as 'Spring 2009'. In addition to this general monitoring exercise, targeted monitoring exercises were carried out in cases where, as a result of his supervision activities, the EDPS became concerned 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. Targeted monitoring and reporting exercises

The EDPS initiated targeted, correspondence-based monitoring exercises in cases where he was concerned about an issue related to compliance with the Regulation in an institution or an agency. This was the case, for example, at the ECB on internal administrative inquiries or on processing operations at DG RELEX.

Internal administrative inquiries - European Central Bank

In January 2010, the EDPS opened an inquiry into the protection of personal data in the process of internal administrative inquiries at the European Central Bank (ECB). This decision was taken on the basis of Article 46(b) of the Regulation, as a follow-up to the EDPS opinion of 22 December 2005 on such inquiries at the ECB. The inquiry focused on possible access to electronic files and the interception of telephone conversations. A number of questions relating to the application of the ECB Administrative Circular 01/2006 on internal administrative inquiries and its principles were sent to the ECB. These included, among others, questions about the way the procedure is documented, the existence or not of a computer forensic protocol as well as annual statistics for the interception of telephone conversations and access to electronic files and traffic data. The inquiry has not yet been concluded.

The Inventory of DG RELEX

As a result of a number of complaints, the EDPS became concerned that the inventory of processing operations under the control of DG RELEX did not accurately reflect the processing operations involving personal data within the EU delegations. The EDPS also wished to confirm that DG RELEX had notified all the processing operations of the EU delegations to the DPO of the Commission in accordance with Article 25. DG RELEX subsequently provided updates and appropriate assurances regarding both these matters and the case was closed.

Visit to the European Network and Information Security Agency

On 17 September 2010, the EDPS visited the European Network and Information Security Agency (ENISA) to verify and discuss the low level of compliance with Regulation (EC) 45/2001. This visit was triggered by evidence gathered during supervision activities by the EDPS, in the form of a complaint, a consultation and the absence of follow-up to a prior checking Opinion.

The visit also allowed the DPO to update the EDPS on ENISA's progress including an e-register, a follow-up mechanism and a new inventory. The DPO underlined the problems of independence in exercising his DPO duties and the Assistant Supervisor mentioned the paper on professional standards for DPOs (since adopted in October 2010) which should help the DPO reinforce and clarify his role internally.

During the closing meeting and based on EDPS requirements, a supervision roadmap (including specific deadlines) was agreed by both parties which emphasised the importance of the three major tools for compliance with the Regulation: the inventory, the register and Article 27 notifications to the EDPS. The EDPS will closely follow the progress made by ENISA in the roadmap subsequently so as to ensure compliance with the Regulation is achieved.

Visit to the European Environment Agency

On 10 December 2010, the EDPS visited the European Environment Agency (EEA) in order to verify and discuss the level of compliance with the Regulation at the Agency.

The visit consisted of a meeting between the EDPS and the Director of the EEA, with further meetings involving the DPO and controllers of processing operations. These provided an opportunity for the EDPS to raise his concerns in relation to the current level of compliance at the EEA and allowed the Agency to update him on their progress towards achieving full compliance. In this context, the EDPS was pleased to note the Agency's significant recent efforts and commitment to addressing its shortcomings.

Both parties agreed on a roadmap of compliance (including specific deadlines) which would be closely monitored by the EDPS.

2.5.2. General monitoring and reporting: 'Spring 2009' exercise

Following the general monitoring exercise launched in spring 2009, the EDPS has continued to monitor the implementation of data protection rules and principles by the institutions and bodies involved.

The **EU institutions** continued to make **good progress** in meeting their data protection requirements and although some other bodies have also made improvements, a **lower level of compliance** was generally found within the **agencies**.

In cases where the EDPS believed that progress towards compliance was insufficient, appropriate targets were set. Unfortunately, in some cases such targets were not met and, as a result, the EDPS requested further updates. Where such updates were still not forthcoming or where progress was too slow, the EDPS launched more targeted monitoring exercises (see above).

Updates in relation to the Spring 2009 exercise

- **Notification of processing operations from data controllers to the DPO**: overall, the level of notifications has risen and whilst the EDPS will continue to seek updates on progress, he will also address under-performing institutions and bodies in accordance with his recently published policy paper on monitoring and ensuring compliance.
- **Notification of processing operations to the EDPS for prior checking**: most of the institutions have made significant progress in this regard, although once again levels of compliance remain lower at agencies and the EDPS will, therefore, seek to address this over the coming year.

2.5.3. Next steps

The EDPS will encourage and closely monitor further progress, in particular in those institutions and agencies where compliance in the field of prior checking by the EDPS and notifications to the DPO need to be improved. He will also continue to emphasise the usefulness of an **inventory** and an internal **follow-up procedure for his recommendations**, in ensuring compliance with the Regulation.

The next general monitoring exercise (**Spring 2011**) will begin in early 2011, although as a result of evidence already gathered in previous exercises, additional targeted initiatives regarding compliance are likely to continue.

2.5.4. Inspections

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

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 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 2010, the EDPS continued the follow-up of previous inspections. In addition, in December 2010, the EDPS carried out an inspection at the Commission's Joint Research Centre (JRC) in Ispra.

Follow-up of the inspection at the European Personnel Selection Office

In March 2009, the EDPS carried out an inspection at the European Personnel Selection Office (EPSO). The inspection sought the facts regarding several processing operations which were the subject of prior checks relating to the selection of officials, temporary staff and contract agents, as well as any related personal data processing operations. The EDPS made a number of conclusions, notably about the transparency of EPSO procedures and the conservation of data, which were subsequently taken into account by EPSO.

The inspection was also aimed at ensuring the compliance of **selected EPSO databases and IT tools** used in the selection procedures. The EDPS is still awaiting further feedback on progress made in the implementation plan for his recommendations. The EDPS has therefore reserved his final conclusions on the inspection, pending receipt of this information.

Follow-up of the inspection at the European Court of Auditors

Following the inspection that the EDPS conducted at the European Court of Auditors (CoA) in March 2009 in relation to **monitoring staff** (Internet monitoring and audit tool report), ongoing collaboration with the Court has been fruitful and progress towards compliance on the topics examined has been noted by the EDPS.

In the **Internet monitoring case** (Case 2008-0284), the EDPS made specific recommendations in his report on the follow-up of the adopted opinion. Further discussions are still taking place to ensure

Inspections are a fundamental tool to monitor and ensure the application of the Data Protection Regulation.

full compliance in the general framework of the analysis of this issue in the institutional context.

Regarding the consultation on a procedure to access private drive/e-mail of staff members, the EDPS concluded that a formal notification for prior checking had to be submitted to him regarding this processing operation, as it gave rise to a specific risk under Article 27(1) of the Regulation. In January 2010, the EDPS delivered his opinion (Case 2009-0620) authorising the processing operations subject to some specific recommendations, which were subsequently implemented by the CoA. Therefore, the EDPS has since closed the case.

Follow-up of the s-TESTA inspection

The s-TESTA (Secure Trans-European Services for Telematics between Administrations) network provides a generic infrastructure to serve the business needs and information exchange requirements of European and national administrations. Currently, more than 30 applications rely on this secure network provided by the European Commission.

In January 2010, the EDPS adopted a report with 22 recommendations related to the inspection conducted previously at the Service and Operational Centre (SOC) of s-TESTA. In December 2010, the Commission sent the EDPS an implementation report regarding these recommendations, indicating that 12 had already been implemented. The remaining 10, which required more significant investment, have been included in the continuous improvement plan of the system and will be finalised in 2011. The EDPS will check these remaining elements in the course of a follow-up action scheduled for mid-2011.

Inspection at the Joint Research Centre

In December 2010, the EDPS carried out an on-the-spot inspection at the Joint Research Centre (JRC) in Ispra. A general lack of cooperation from the JRC, coupled with the need to check the reality and verify the implementation of his recommendations *in-situ*, triggered the decision to carry out the inspection.

Two main areas were inspected: the selection and recruitment of JRC personnel, and the procedures put in place by the security service (pre-employment security check, security investigations, access control and recording of emergency calls). In all these cases, background information had been provided by prior checking analyses.

During the inspection, collaboration between the EDPS and the relevant units of the JRC was productive and enabled the inspectors to conclude, among other things, that communication issues were the main cause of the previous lack of cooperation. Based on the findings, the EDPS will issue an inspection report with new recommendations to ensure better compliance with the Regulation.

2.6. Consultations on Administrative measures

2.6.1. Consultations Article 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' has 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 for a very wide material scope for the 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 have been examined, some of which are reported below.

2.6.2. Request for access to the identity of an informant - European Ombudsman

The European Ombudsman consulted the EDPS on an issue raised in a complaint lodged against OLAF. The consultation included a number of questions, such as:

- whether the identity of the persons who provide OLAF with information, as informants or whistleblowers, should not be disclosed to anyone other than the judicial authorities;
- whether the protection of informants and whistleblowers has to be guaranteed after the closure of an investigation where there is no follow-up and, if so, in what way and to what extent.

The EDPS provided comments at rule or policy level, rather than in relation to the specific complaint against OLAF. The EDPS took the position that, as a general rule, the identity of a whistleblower or informant should not be disclosed, except when this would contravene national rules on judicial procedures and/or where they maliciously make a false statement. In such cases, these personal data could only be disclosed to judicial authorities.

As to the second question, the EDPS considered that there are good reasons to believe that the protection of whistleblowers and informants should be the same after the closure of an investigation, regardless of whether there is a follow-up or not. The vulnerability of the whistleblower's or informant's role and, therefore, the risks to their privacy and integrity do not change depending on whether the investigation is opened or closed with no follow-up.

In practice, this approach would of course not exclude situations where the protection of whistleblowers or informants should be superseded by the legitimate claims of others. The passage of time may be a relevant factor, but it is obviously difficult to speculate about this in the abstract.

2.6.3. International transfers of personal data - European Aviation Safety Agency

The European Aviation Safety Agency (EASA) performs some activities (e.g. services in the field of certification) that give rise to the payment of fees and charges by applicants. Part of these certification activities may be conducted fully or partly outside the territory of the Member States. In some cases, the Agency has been asked by the applicants to provide them with the names and date of travelling of the experts in order to allow them to proceed with the payment of the invoice.

The DPO of EASA asked the advice of the EDPS on the application of Article 9 of the Regulation to the case under consideration.

According to Article 9.1 personal data shall only be transferred to recipients, other than EU institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, **if an adequate level of protection is ensured** in the country of the recipient.

The EDPS underlined that, if the third country in question – outside the EEA – does not ensure an adequate level of protection, the other conditions mentioned in Article 9 should be taken into account. Article 9.6 stipulates that 'by way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (...) (d) the transfer is necessary or legally required on important public interest grounds (...)'.

Since the performance of the services in this case is one of the core activities of EASA, the transfers conducted for the payment of those services could be considered, in principle, as **necessary for the functioning of this body**, so as to qualify for derogation under Article 9.6 (d).

The EDPS also noted that, in the present case, it appeared that transfers would not be 'repeated, mass or structural', but take place as a 'one off' transfer to different recipients in different countries. As to the risks to the data subjects, no specific risks had been mentioned. The categories of data to be transferred (the name and travel date of the given experts) did not seem to give rise to particular concerns either.

The EDPS pointed out, however, that no safeguards were established in those cases where an exception was applied. For this reason, he recommended the inclusion of a clause that should specify that the recipient is legally authorised to request this data and limit the use of the data to the sole purposes motivating the transfer.

2.6.4. Policy on the internal use of email - European Commission

The European Commission consulted the EDPS regarding its policy on the internal use of email.

The EDPS analysed specific points of the policy in terms of personal data protection and privacy principles, as well as security measures.

In this context, the Commission informed the EDPS that it does not conduct large scale monitoring at an individual level. A letter sent to the EDPS stated that *'[t]he only form of routine monitoring that takes place by the email service of the Commission (DG DIGIT) is at the DG/service level and not at the level of individual mailboxes or individual traffic data level. DG DIGIT monitors the usage in order to reduce operational threats, but no routine reports are produced that monitor individual mailbox activity or provide any individual traffic data that can be used for analysis of individual abuse'*.

This implies that any individual mailbox monitoring could **only** take place **as part of an ongoing investigation**. The EDPS welcomed this approach which he considers to be the best practice.

2.6.5. IT administrator rights - European Investment Bank

On 26 March 2010, the EDPS replied to a consultation from the European Investment Bank (EIB) with recommendations regarding the management of IT administrators' access to personal data stored in IT systems and applications. The EDPS underlined the need to apply the **principle of segregation of duties**. The degree of segregation should be defined in light of the level of risk identified for the related process.

The management of IT administrator access rights should be addressed through a balanced approach between organisational and technical measures. The EDPS also recommended that these measures be properly documented in a detailed security policy established by the institution.

2.6.6. Monitoring of telephone communications

The EDPS was consulted on a project involving the monitoring of telephone communications which are above a predefined threshold.

The system envisaged was based on a predetermined threshold (tolerated number of hours or tolerated cost of telephone communications) that would be offered to staff. At the end of each month, the managers would receive a list of the users working for him/her and whose communications relating to calls abroad or to mobile phones (private and/or professional) have exceeded the threshold during the past month.

The monitoring of the use of the phone for private purposes could in principle be considered as a breach of the right to privacy of staff members.

The EDPS recognised that the lawfulness of processing of such data is covered by the legitimate exercise of the official authority vested in the institution or body to efficiently manage the use of telecommunication tools within the institution or body (Article 5a of the Regulation supported by the provisions in Article 37(2)). However, the EDPS also considered that monitoring across the board, as opposed to a more selective monitoring, is not necessary at all times.

Although the EDPS accepted the legitimate purpose of budget management, he considered that the monitoring of the use of the phone for private purposes, even without communication of the details of the calls made, could possibly be considered as a breach of the right to privacy of staff members.

In this respect, the EDPS requested that the institution or body ensure that the threshold figure which would trigger the sending of a list to the management, is sufficiently high so as to avoid non-justified monitoring and enables the identification only of those cases in which there is clear or repeated abuse of the system. The institution or body was also invited to examine the extent to which other indicators could be used to identify possible abuses.

The EDPS therefore invited the institution to reassess the proposed system and to examine whether other less intrusive methods could be used.

2.6.7. Further processing of data for transfers to AMEX - European Food Safety Agency

The European Food Safety Agency (EFSA) processes annual Declarations of Interests (DoI) of certain persons engaged in the activities of EFSA for the purpose of verifying that these persons have no conflict of interests which could interfere with the activities they carry out for EFSA.

In the course of the prior checking of these data processing operations (Case 2008-0737), the DPO of EFSA asked the advice of the EDPS on the further use of the DoI database for the purpose of providing its travel agency, AMEX, with the identification data of external experts.

The DPO of EFSA asked the EDPS whether the further processing of the data included in the DoI database for the purpose of providing the travel agency with the identification data of external experts would respect Article 4(1)(b) of the Regulation.

According to this provision, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

In his opinion, the EDPS concluded that any further processing by EFSA of data processed in the DoI database, for the purpose of providing the identification data of persons who can benefit from AMEX travel services, would serve a totally **different purpose** which would not be considered compatible with the initial purpose of the data collection and processing. Therefore, such further processing by EFSA would not comply with Article 4(1)(b) of the Regulation.

The EDPS further pointed out that the role and responsibilities of AMEX in respect of the data are not made sufficiently clear in the data protection covenant entered into between the parties; in particular the reasons why, and in which circumstances, AMEX acts as a processor and/or as a controller are not clear. Proper guarantees should be in place to ensure the rights of the data subjects and to secure onward transfers by AMEX to other recipients, in accordance with applicable data protection laws.

2.6.8. Retention periods for medical documents - Board of Heads of Administration

In November 2006, the President of the Board of Heads of Administration (the Board) sought the opinion of the EDPS on a note prepared by the Commission on the retention periods of some medical documents. The EDPS issued an opinion on 26 February 2007 underlining that the 30 year period indicated in the note should not constitute the *minimum* data conservation period for medical documents. On the contrary, with some limited exceptions, it should be regarded as the *maximum* data conservation period. Furthermore, the EDPS considered that application of the rule in Article 4 of the Regulation means that the nature of the medical documents should be examined in order to determine what conservation periods would be suitable to each type of document.

The issue of the conservation of medical documents was raised again in September 2010, when the *Comité de Préparation pour les Affaires Sociales* (the CPAS), the relevant sub-committee of the

The 30 year conservation period of medical documents should be considered as a maximum conservation period.

Board, prepared a report on a number of different cases with specific retention periods of medical documents. In October 2010, the Board consulted the EDPS on this report. The EDPS is currently examining the issue and will issue his position on the consultation taking into account his opinion of February 2007 and his position in previous prior-checking opinions.

2.6.9. Implementing rules concerning the Data Protection Officer

*The Data Protection Regulation requires that further **implementing rules concerning the tasks, duties and powers of the DPO** be adopted by each EU institution or body. In July 2010, the EDPS issued **guidelines** to facilitate the drafting of implementing rules where these have not yet been adopted or where they need to be revised.*

In May 2010, the European Research Council Executive Agency (ERCEA) submitted its implementation rules on the function of the DPO to the EDPS for consultation. These rules also covered the role of controllers and the rules pursuant to which a data subject may exercise his rights. The EDPS welcomed this inclusive approach all the more since ERCEA also took on board the best practices suggested over the years by the EDPS such as:

- keeping an anonymous inventory of the written requests from a data subject to exercise a right (access, rectification, blocking, etc.);
- collaborating with IT and Information Security services of the Agency to supplement the DPO sources of information.

The European Network Information Security Agency (ENISA) and the Court of Auditors also submitted the revised version of their implementing rules for consultation to the EDPS. These consultations were in line with the guidelines issued by the EDPS.

2.7. Thematic guidelines

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 the field of recruitment, health data, administrative enquiries and disciplinary proceedings and video surveillance. The EDPS is currently working on guidelines for staff evaluation and processing of personal data in anti-harassment procedures.

2.7.1. Guidelines on administrative enquiries and disciplinary proceedings

In April 2010 the EDPS issued guidelines on the processing of personal data in administrative inquiries and disciplinary proceedings by EU institutions and bodies.

The objective of the guidelines is to harmonise good practice in this field and facilitate compliance with the provisions of the Regulation. The guidelines present in a clear and concise way, the outcome of the EDPS positions as they have been examined in the prior checking opinions. They also set up a number of recommendations regarding each fundamental principle of the Regulation.

One important recommendation concerns the **right of access and rectification** of a data subject. While these rights may be occasionally restricted, the data controller should ensure that such restrictions are necessary and are decided on a case-by-case basis. Furthermore, the controller should ensure that the rights of access and rectification as well as the right to information are guaranteed by other means.

The EDPS also pointed out the lack of a harmonised approach to the **retention period of disciplinary data** which leads to conflicts with the data protection principles and other fundamental rights of the data subject. This is due to some significant gaps in Annex IX to the Staff Regulations and the absence of a common policy among the EU institutions and bodies on conservation of such data.

Finally, the EDPS underlined the need for further consideration of the specific issue of **interception of communications**, with particular emphasis on the legal basis of tapping voice communications and the possibility of doing this without a judicial warrant or authorisation.

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 next step will be for the EDPS to issue a joint opinion on notifications submitted by the agencies for prior-checking in the light of the guidelines.

2.7.2. Guidelines on video-surveillance

In March 2010, the EDPS issued a practical set of guidelines to EU institutions and bodies on how to use video-surveillance responsibly with effective safeguards in place. The guidelines set out the principles for evaluating the need for resorting to video-surveillance and give guidance on how to do so in a way which minimises the impact on privacy and other fundamental rights.

A consultation draft was published in July 2009 as was reported in the EDPS Annual Report for 2009. The consultation process elicited feedback on improving the draft guidelines and increasing cooperation with stakeholders.

EU institutions have until 1 January 2011 to demonstrate compliance with EDPS Guidelines.

The guidelines indicate that decisions on whether to install cameras and how to use them should not be based solely on security needs. Rather, **security needs must be balanced against the fundamental rights of an individual**. With that said, fundamental rights and security do not have to be mutually exclusive. Using a pragmatic approach based on the principles of selectivity and proportionality, video-surveillance systems can meet security needs whilst also respecting privacy.

Within the limits provided by data protection law, each institution and body has a margin of discretion on how to design its own system. The guidelines are designed to allow customisation. This flexibility should prevent a rigid or bureaucratic interpretation of data protection concerns from hampering justified security needs or other legitimate objectives.

At the same time, each institution must also **demonstrate that procedures are in place to ensure compliance** with data protection requirements. Recommended organisational practices include adopting a set of data protection safeguards that are to be outlined in the institution's video-surveillance policy and periodic audits to verify compliance. Impact assessments carried out by the institutions are encouraged, whereas prior checking by the EDPS will still be required for video-surveillance involving great inherent risks (such as covert surveillance or complex, dynamic-preventive surveillance systems).

Transition period

The guidelines apply to existing as well as future systems: each institution had until 1 January 2011 to bring its existing practices into compliance. The EDPS continued to be available when further advice was needed on specific issues.

The EDPS also assisted those institutions that had already submitted their prior checking notifications before the issuance of the guidelines. There were nine such cases. In July 2010, the EDPS issued preliminary recommendations in these cases, with the understanding that compliance with these recommendations could not be considered as a substitute of an institution's own in-depth internal analysis of the guidelines, its practices, and its compliance status. The EDPS comments were to assist the institutions concerned in focusing their attention on the key items to be addressed. Issues requiring specific attention included covert surveillance and retention periods.

In a similar vein, the EDPS also issued preliminary guidance to OLAF whose video-surveillance system is the only one that the EDPS had prior checked before the issuance of the guidelines (on the grounds that it was a true prior checking notification involving a new system and therefore, had to be dealt with as a priority).

The EDPS also continued to provide guidance to other institutions with respect to the interpretation and implementation of the guidelines, and continued to handle complaints and consultations, including a complaint against covert surveillance practices in one institution and an administrative enquiry concerning the restrictions on the use of video-surveillance footage as evidence if it was obtained in breach of data protection rules.

2.8. The EDPS compliance and enforcement policy

In December 2010, the EDPS adopted a policy paper entitled 'Monitoring and Ensuring Compliance with Regulation (EC) No 45/2001'.

This policy signals a fundamental change of gear in relation to enforcement of the Regulation. To date, the EDPS has preferred to make recommendations and encourage compliance, rather than warn or admonish controllers or make legally binding orders. Following five years of such activity, the EDPS believes that the time has come to take a more **robust approach to enforcement**, particularly in cases of serious, deliberate or repeated non-compliance with data protection principles. The policy therefore introduces a set of criteria which will ensure a proactive, as well as consistent and transparent, application of his enforcement powers.

The paper sets out the framework within which the EDPS monitors, measures and ensures data protection compliance in the EU administration. It explains the nature of the various enforcement powers available to the EDPS and outlines the drivers and triggers for any formal action that he might take.

The policy seeks to **encourage voluntary compliance and best practices** and create sufficient incentives for compliance by:

- emphasising where the responsibility for compliance lies;

The EDPS believes that the time has now come for a more robust approach to enforcement.

- explaining how the EDPS will support this compliance;
- explaining what the EDPS will do in the case of non-compliance.

The policy also places a strong emphasis on the **principle of 'accountability'** to encourage compliance and the adoption of best practices within the EU administration. Accountability requires the EU institutions and bodies and data controllers acting on their behalf, to put appropriate and effective measures in place to ensure compliance with data protection obligations and to subsequently demonstrate this to the EDPS.

Lastly, the paper outlines the approach of the EDPS to **transparency and publicity** in relation to his enforcement activities, emphasising that these are important tools both for stakeholders and in terms of good governance. Therefore, in future the EDPS will normally publish information regarding any official referrals he makes to the Parliament, the Council, the Commission or the Court of Justice. In addition, he will also consider, on a case-by-case basis, whether it is appropriate to make public any of his other enforcement activities.

The EDPS hopes that by enabling him to focus on his responsibilities for monitoring and ensuring compliance through a selective, targeted, risk-based approach to enforcement, this policy paper will facilitate a more efficient and effective use of the resources of the EDPS.

3 CONSULTATION

3.1. Introduction: overview of the year and main trends

In 2010, the Commission made significant progress towards a new, **modernised legal framework for data protection in Europe**. The public consultation launched in 2009 was concluded and supplemented by further targeted consultations with a number of key stakeholders.

In November 2010, the Commission issued its Communication laying down a comprehensive approach on personal data protection in the European Union, identifying the main priorities and key objectives for the review of the current rules.

This project has been high on the EDPS agenda for 2010 and will be one of his main priorities for the coming years.

In 2010 the Commission and the Council also devoted significant efforts to the **implementation of the Stockholm Programme** – an open and secure Europe serving and protecting the citizen, adopted by the European Council in December 2009. The Programme defines strategic guidelines for legislative and operational planning within the area of freedom, security and justice and focuses on the interests and needs of citizens.

*The Stockholm Programme emphasised that **security and law enforcement measures and respect for fundamental rights, including data protection, must go hand in hand**. It also recognised the need to protect personal data in a global society which is characterised by rapid technological change and borderless information exchange.*

Several initiatives directly connected with the implementation of the Stockholm Programme were closely monitored by the EDPS. Among other things, the EDPS dealt with critical data protection issues related to the EU Internal Security Strategy, information management in the area of freedom, security and justice and the EU Counter-Terrorism Policy. All in all, developments in connection with the Stockholm Programme have been dominant items in the EDPS agenda and will remain so for the next few years.

The **interface between privacy and technological developments** was also an area in which the EDPS intervened significantly. In May 2010, the Commission published its Communication on a Digital Agenda for Europe, with the objective of setting EU priorities in the field of the Internet and digital technologies. Several of these initiatives have significant data protection relevance and are closely monitored by the EDPS. The EDPS is also convinced that new technologies do not just pose new challenges for privacy and data protection, but also offer new opportunities for protecting personal data.

It is, therefore, essential that privacy requirements are embedded into the design, operation and management of ICT systems across the entire information life cycle. The EDPS thus strongly advocates the inclusion of the 'privacy by design' principle in the new legal framework.

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

The EDPS was also consulted on initiatives in the field of **international cooperation on security and law enforcement**, such as the EU-US general agreement on data sharing for law enforcement purposes and the agreement on the exchange of financial data for the purposes of the Terrorist Finance Tracking Program (TFTP). He also intervened with regard to the Anti-Counterfeiting Trade Agreement (ACTA) and several agreements on the exchange of Passenger Name Records (PNRs).

The EDPS was also active in other areas, such as the large-scale data exchanges taking place in the context of the Internal Market Information System, the use of security scanners at airports and cooperation in the field of taxation.

The wide diversity of policy areas in which the EDPS is consulted further demonstrates that data processing has become an increasingly fundamental element of a high number of legislative initiatives. These initiatives often raise significant data protection issues and, as a result, further justify the role of the EDPS as an advisor to the EU institutions.

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' ([8]) remains relevant, although it must now be read in the light of the Lisbon Treaty.

As a rule, the EDPS 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 a quick and fundamental political message or to focus on one or more technical aspects, or even to summarise or repeat observations made earlier.

Other instruments can also be used, such as oral presentations, explanatory letters, press conferences or press releases. For instance, in 2010 the EDPS held a press conference on the 'Future of the EU legal framework for data protection' in combination with the presentation of the 2009 Annual Report.

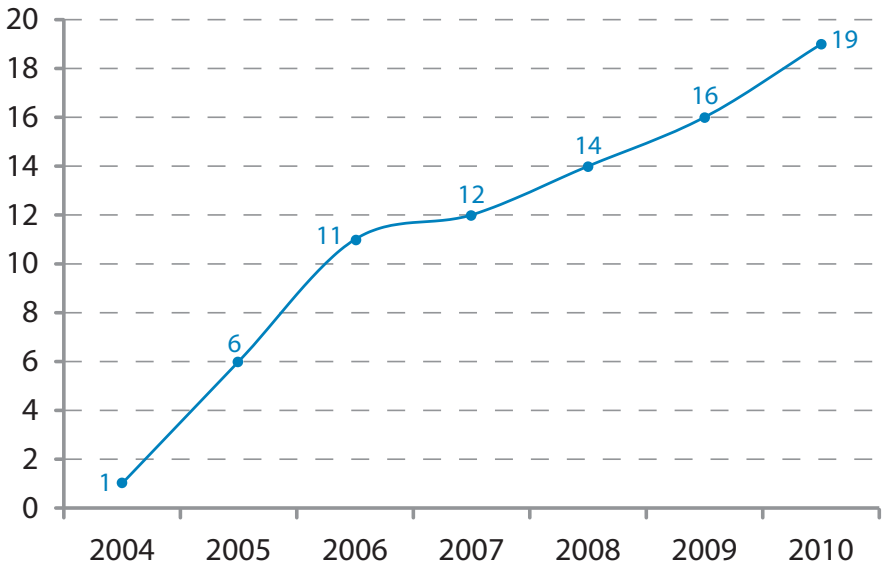
The EDPS is available during all phases of policy making and legislation and uses a wide range of other instruments in his advisory role. Although this may require close contact with EU institutions, safeguarding his independence remains a paramount concern.

Contact with the Commission takes place at various stages of the preparation of proposals, and the intensity 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 e–Justice initiative or the review of the data protection framework to which the EDPS contributed at different stages.

Regular contacts with the relevant institutions' services in the follow-up phase also took place. In some cases, the EDPS and his staff were closely involved in the discussions and negotiations in Parliament and the Council. In other cases the Commission was the main interlocutor in the follow up phase. The legislative process on the Frontex-regulation, the follow-up of the Digital Agenda (for instance on the issue of net neutrality) and the Internal Market Information System are further examples of intensive involvement leading to further comments by the EDPS in 2010.

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

Legislative opinions evolution 2004-2010

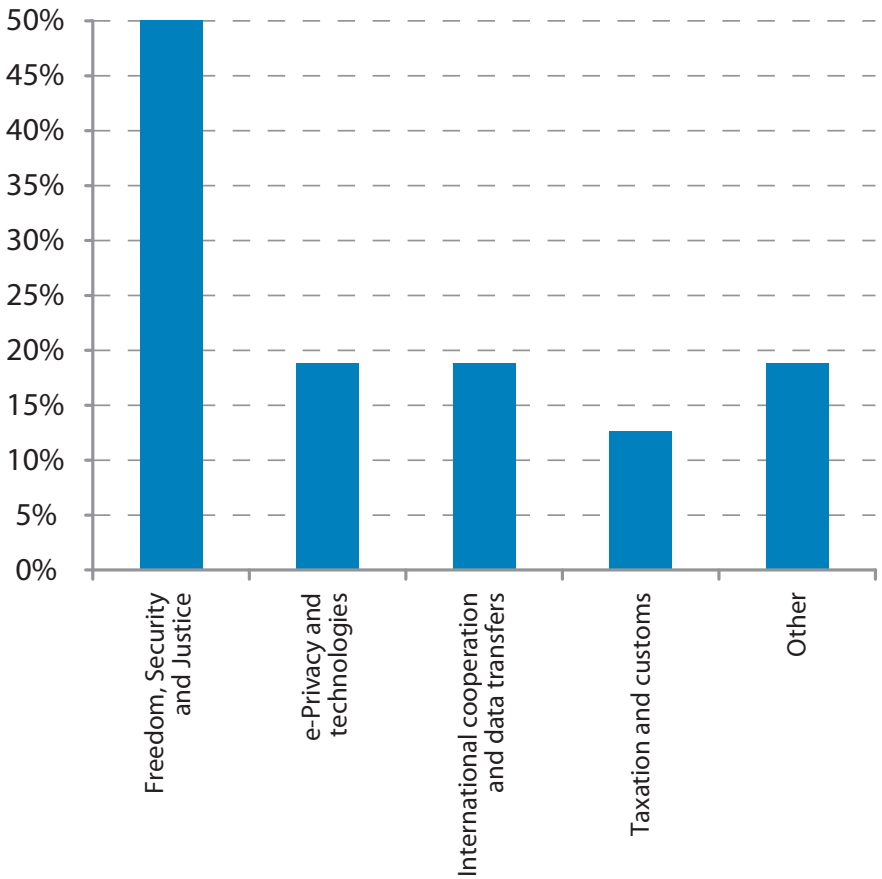


3.2.2. Results of 2010

In 2010 the steady increase in the number of opinions continued. The EDPS issued 19 opinions on a wide variety of subjects.

With these opinions and the other instruments used for intervention, the EDPS implemented the priorities for 2010, as laid down in his Inventory. The 19 opinions covered different EU policy areas.

Main policy areas for legislative opinions in 2010



The 2010 Inventory defined four main areas of attention:

- The new legal framework for data protection;
- Freedom, Security and Justice;
- International cooperation and data transfers;
- Technological developments.

The EDPS focused extensively on all these areas in 2010. In keeping with the 2010 Inventory, the EDPS concentrated mainly on those initiatives which had been given high priority in the Inventory (i.e. the red initiatives): the EDPS issued an opinion or otherwise reacted in 13 out of the 15 high-priority proposals which were adopted in the course of 2010.([9])

The content of the EDPS' opinions and other contributions in the field of consultation are described in further detail below.

3.3. Review of the EU Data Protection Framework

The review of the EU legal framework for data protection was already one of the top priorities for the EDPS in 2009, when debate over the reform officially started. In 2010, interest in the reform intensified significantly with the publication in November 2010 of the Commission Communication laying down a comprehensive approach on personal data protection in the EU. The EDPS gave special attention to this issue throughout 2010 and conveyed his messages in various ways.

([9]) In two of these cases (Revision of Regulation (EC) No 831/2002 on access to confidential data for research purposes and Council Framework Decision on attacks against information systems), an opinion was not considered necessary at this stage.

The new data protection framework must be ambitious and actually enhance the effectiveness of the instruments of data protection in a globalised and technologically driven society.

The EDPS held an *ad hoc* **press conference** immediately after the publication of the Communication to publicly express his views on the new legal framework. On this occasion, he emphasised the importance of the review, which he considered to be very timely and gave his point of view on the main points of the new framework.

*The EDPS insisted on the need for **strong and effective data protection** in a society where personal information is used in quantities that cannot be measured, very often without individuals being aware of it. The EDPS welcomed the Commission Communication, but warned that there was **no room for mistakes**: the challenges are enormous and the proposed solutions have to be equally **ambitious** and enhance the effectiveness of data protection instruments.*

The EDPS also gave his views on the main points for the new framework. He highlighted in particular:

- his support for achieving **further harmonisation** of national data protection legislation;
- the need for a **technologically neutral** approach;
- the inclusion of the principles of **privacy by design and accountability**;
- the introduction of a **mandatory security breach notification** covering all relevant sectors;
- the **inclusion** of the **areas of police and justice** in the general framework.

The EDPS has elaborated further on these views in a comprehensive opinion adopted in January 2011.

The Commission is expected to adopt a fully-fledged legislative proposal in the course of 2011. The EDPS will continue to monitor the legislative process closely in 2011 and will issue further contributions as appropriate.

3.4. Area of freedom, security and justice

During 2010, the EDPS followed the developments in connection with the implementation of the **Stockholm Programme** with great attention and issued recommendations on a number of legislative and non-legislative initiatives directly or indirectly related to the area of freedom, security and justice.

3.4.1. EU Internal Security Strategy

The EU Internal Security Strategy (ISS) lays out a European security model to integrate action on law enforcement and judicial cooperation, border management and civil protection. The ISS, approved by the Council in February 2010 and endorsed by the European Council a month later, was followed by a Commission Communication in November 2010 targeting the most urgent security threats facing the EU, such as organised crime, terrorism, cybercrime, the management of EU external borders and civil disasters.

Due to the **potentially intrusive** nature of the measures to be taken under the Strategy, the EDPS followed the discussions on the ISS closely and the actions envisaged to implement it. In his opinion adopted in December 2010, the EDPS emphasised the need to ensure the **right balance** between the objective of ensuring the safety of citizens and the efficient protection of their privacy and personal data. The EDPS also drew attention to the fact that the ISS presents obvious **policy links with other EU strategies** currently being developed at EU level, such as the Information Management Strategy and the review of the EU data protection legal framework.

The EDPS called for an efficient Internal Security Strategy supported by a solid data protection scheme complementing it.

The EDPS called for a **more comprehensive and integrated approach to the ISS** providing for explicit links and interactions between the different initiatives concerned. He took the position that an efficient ISS could not be put in place without the support of a solid data protection scheme complementing it.

3.4.2. Information management

The Stockholm Programme invited the Commission to assess the need for developing a **European Information Exchange Model** based on the evaluation of the current information exchange instruments. The Programme also referred to **a strong data protection regime** as the main pre-requisite for the EU Information Management Strategy. In July 2010, the Commission adopted a **Communication on the overview of information management** in the area of freedom, security and justice, on which the EDPS issued an opinion in September 2010.

The EDPS fully supported the ongoing work on the evaluation of all instruments dealing with information management in the area of freedom, security and justice. He emphasised the fact that this initiative was a **first step in the evaluation process** and urged that there be an **objective, comprehensive and in-depth assessment** of all existing instruments to be used in the framework of the Information Management Strategy before proposing new ones.

The EDPS also suggested reporting and taking into consideration the deficiencies and weaknesses of the systems in future work on information management.

3.4.3. FRONTEX

In February 2010, the Commission put forward a **proposal revising the legal framework governing FRONTEX** in order to strengthen the operational capabilities of the agency. In the opinion issued in May 2010, the EDPS focused on the growing tasks of the agency and their consequences for data protection.

The EDPS was particularly critical about the fact that the proposal did not specify whether and to which extent FRONTEX would be allowed to process personal data. The EDPS called on the legislator to lay down clear rules on data protection and provide for a clarification of the conditions and circumstances under which data processing by FRONTEX could take place.

The EDPS also monitored the discussions on this dossier in the European Parliament closely. In a letter addressed to the European Parliament's Rapporteur, he made concrete suggestions aimed at introducing a **specific legal basis** dealing with this issue the proposal, which will be subject to **strong data protection safeguards** and in accordance with the principles of proportionality and necessity.

3.4.4. Counter-terrorism policy

The fight against terrorism is an area where personal data are often processed in a broad and preventive way.

In his opinion on the EU Counter-Terrorism policy, the EDPS called for **concrete initiatives** supporting the respect of fundamental rights in this area, particularly the right to the protection of personal data. The EDPS stressed the need to ensure **consistency** and clear relations between all policies and initiatives in the area of home affairs and internal security. He also recommended that the EU legislator **step up the role of data protection in this area**. In particular, the **principle of necessity** should be explicitly considered in each proposal. This ought, accordingly, to prevent possible overlaps with existing instruments from occurring and the collection and exchange of personal data should, moreover, be limited to what is really necessary for the purposes pursued.

In addition, a comprehensive and global approach should be proposed with regard to **asset-freezing measures** directed at specific countries and suspected terrorists, with a view to ensuring both the effectiveness of law enforcement actions and respect for fundamental rights. With regard to international cooperation, the EDPS recalled the need to ensure that adequate safeguards be put in place when personal data are exchanged with third countries and international organisations, so that the data protection rights of citizens are adequately respected in this context.

3.4.5. Marketing and use of explosives precursors

From a data protection point of view, the collection of data regarding suspicious transactions in certain chemicals is the most sensitive subject in the Commission proposal for a Regulation on the marketing and use of explosives precursors. The main aim of the proposal is to reduce the risk of attacks by terrorists or other criminals using home-made explosive devices. The EDPS called for clarification of the relevant provisions so as to ensure that the **data processing remains proportionate and abuse is prevented**.

Ensuring a high level of data protection also contributes to fighting racism, xenophobia and discrimination, which, in turn, can contribute to preventing radicalisation and recruitment into terrorism.

The main EDPS recommendations were that:

- **data should not be used for any other purpose** than the fight against terrorism (and other crime involving the misuse of chemicals for home-made explosive devices);
- **data should not be retained for long periods of time**, especially if there are a large number of potential or actual recipients or if the data

Personal data linked to unconfirmed suspicions of terrorist activities should not be stored indefinitely

were to be used for data mining. This is even more important in those cases where it can be shown that the initial suspicion was unfounded. The EDPS called for the Regulation to specify a maximum retention period (*prima facie,* not exceeding two years) for all personal data regarding reported suspicious transactions;

- **processing of special categories of data should be expressly prohibited**, in order to prevent discriminatory practices such as profiling based on race or religion.

3.4.6. Eurodac Regulation

In his opinion published in December 2010, the EDPS focused on the problem of '**failure to enrol**' (which in this precise context means the impossibility for an asylum seeker to provide readable fingerprints). The EDPS insisted on the principle that failure to enrol should not by itself lead to a denial of rights for asylum seekers. In particular, he firmly rejected the presumption that a person who has unreadable fingerprints - *ipso facto* - has tried to frustrate the identification procedure, for instance by self-mutilation.

The opinion also welcomed the fact that the possibility of giving **law enforcement agencies access to EURODAC,** had been **left out of the current proposal**.

The EDPS made recommendations concerning information of the data subject: the precarious position of asylum seekers or illegal immigrants was all the more reason to provide accurate and helpful information on their rights. The opinion also covered the use of best available techniques as a way to implement 'Privacy by Design' and the consequences of subcontracting (part of) the development or management of the system to a third party.

The EDPS had already contributed several opinions in this area. The recommendations made in this opinion were either based on new developments or on recommendations previously made and not yet taken on board.

3.4.7. Sexual abuse of children and child pornography

In May 2010, the EDPS adopted an opinion on a Commission proposal for a Directive on combating the sexual abuse and sexual exploitation of children and child pornography.

In the opinion, the EDPS insisted on the need to ensure **legal certainty** with regard to all parties involved, including Internet Service Providers (ISPs), victims and individuals using the network.

Although the proposal mentioned the need to take into account the fundamental rights of end users, the EDPS considered that an obligation on Member States to ensure **harmonised, clear and detailed procedures** under the **supervision of independent public authorities** when fighting illegal content, should be added to the proposal.

The EDPS did not question the need to put in place a better framework providing for adequate measures to protect children against abuse. He nevertheless stressed the **impact** of some of the measures, such as the blocking of websites and the setting-up of hotlines, **on the fundamental rights to privacy and data protection** of the individuals involved. The issue raised was not specific to the fight against child abuse, but to any initiative aiming at the collaboration of the private sector for law enforcement purposes.

3.4.8. European Protection Order and European Investigation Order

The initiatives of a number of Member States for a Directive on the European Protection Order (EPO) and the European Investigation Order (EIO) are rooted in the Stockholm Programme and provide for the exchange of personal data between the Member States concerned. While the EPO aims to improve the protection of victims of criminal acts (particularly women), the EIO aims to create a single, efficient and flexible instrument for obtaining evidence located in another EU Member State.

In his opinion, the EDPS emphasised that the processing of personal data, particularly in the sensitive area of freedom, security and justice, must be in conformity with the EU rules on data protection.

Effective protection of personal data is not only important for data subjects but also contributes to the success of judicial cooperation itself, reinforcing judicial cooperation based on mutual recognition and improved data quality in the exchange of information.

Among various recommendations, the EDPS called for the introduction of adequate safeguards to ensure the protection of individuals with regard to the processing of personal data, procedural fairness and the proper observance of confidentiality and professional secrecy provisions. In particular, the EDPS stressed the need to ensure that 1) authentication systems allow only authorised individuals to have access to personal data 2) tracking of accesses and operations be conducted and 3) audit controls be implemented.

This opinion was also an important opportunity for the EDPS to underline the need to establish **specific procedures** to ensure that **consultation of the EDPS also** takes place in cases where an initiative introduced by a Member State relates to the processing of personal data.

3.5. e-Privacy and Technologies

3.5.1. Promoting Trust in the Information Society

In May 2010, the European Commission adopted the Digital Agenda, a strategy comprising a set of policies and actions to boost the digital economy by 2020. The EDPS adopted an opinion on 'Promoting trust in the information society by fostering data protection and privacy' as an input to such a strategy in March 2010.

The opinion emphasised that consumer trust is a key factor in the emergence and successful deployment of Information and Communication Technologies (ICTs), of which Radio Frequency Identification (RFID), social networks, e-Health and e-Transport are just a few examples.

Trust can only be generated if ICTs are reliable, secure, and under the individual's control and if the protection of their personal data and privacy is guaranteed.

The EU has a strong data protection regulatory framework which, in principle, should ensure the protection of the personal data of individuals. However, in many instances, ICTs raise new concerns that are not accounted for within the existing framework. The opinion discussed the measures that could be either undertaken or promoted by the EU to strengthen this framework. In particularl, the EDPS called on the European Commission to take the following courses of action:

- include the principle of **'Privacy by Design'** as a **general binding principle** into the existing data protection legal framework. Privacy by Design should also be fully endorsed by the European Digital Agenda and become a binding principle in future EU policies, for example in e-Transport, e-Goverment, etc.;

- implement the principle of Privacy by Design following a specific approach in three ICT **areas presenting specific risks** to privacy and data protection: a) **RFID**: propose legislative measures regulating the main issues of RFID usage in case self-regulation does not deliver the expected results (e.g. to provide for the opt-in principle at the point of sale) b) **Social networks**: provide for mandatory privacy-by-default settings; c) **Targeted advertising**: where browsers are provided with privacy-by-default settings to facilitate obtaining their consent to receive advertisements.

3.5.2. Internet and net neutrality

In June 2010, DG INFSO opened a public consultation on open Internet and net neutrality in Europe. The consultation raised a number of questions related to traffic management policies which enable network operators and ISPs to handle traffic in a particular way.

In response to the consultation, the EDPS provided comments to highlight to DG INFSO, the data protection and privacy issues that arise when ISPs and network operators engage in traffic management practices.

The EDPS highlighted two aspects related to the implementation of traffic management mechanisms: firstly, it enables providers to examine the content of messages or transmissions and secondly, it gives them the possibility of attributing this information to a particular user. The EDPS underlined the need to take due account of the EU data protection regulatory framework to engage in such actions. More particularly he recalled that the EU data protection framework requires users to have **freely given informed consent** and he gave practical guidance on the requirements for obtaining such consent.

3.5.3. Data Retention Directive

During a conference organised by the Commission in December 2010, the EDPS gave a speech – referring to the 'Moment of Truth' for the Data Retention Directive - in which he argued in favour of seizing the opportunity to **clearly demonstrate the necessity and justification** for the Directive.

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

The EDPS underlined that such a massive invasion of privacy 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 have been achieved with other less intrusive means.

A new or modified EU instrument on data retention should be clear about its scope and create legal certainty for citizens. This means that it should also regulate the opportunities for access and further use by law enforcement authorities and leave no room for Member States to use the data for additional purposes.

Ruling of the German Constitutional Court

On 2 March 2010, the German Constitutional Court **ruled against the German law which implemented the Data Retention Directive**. The German Court considered that use of the stored data should have been made subject to stricter requirements than provided for by the German legislator. In its judgment the Court subsequently formulated criteria for more restrictive access to and use of the data. These criteria would have to be included in German national legislation in order to ensure that the data retention obligation could be implemented without breaching the fundamental rights contained in the German Constitution.

In a statement to the press, the EDPS underlined that the judgment should be seen as an authoritative source of inspiration for other EU Member States and as valuable input for the evaluation of the Data Retention Directive, particularly in light of the new legal framework established by the Treaty of Lisbon.

3.5.4. e-Waste

Privacy and data protection are inherently related to security measures regarding devices capable of storing an increasing quantity of personal data. The EDPS emphasised this aspect in his opinion of April 2010 on the Commission proposal for the recast of the Directive on waste electrical and electronic equipment (also referred to as *e-waste*).

Data retention: the EDPS called upon the Commission to prove the necessity of retaining communication data on such a large scale.

While supporting the proposal's objective of improving environmentally-friendly policies in the area of e-waste, the EDPS nevertheless pointed out that the initiative only focused on the environmental risks related to the disposal of e-waste and did not take into account the **data protection risks** that may arise from the **inappropriate disposal, reuse or recycling** of electrical and electronic equipment waste.

An increased risk of loss and dispersion of personal data exists when personal data relating to the users of the devices and/or third parties remain stored in IT and telecommunications equipment (e.g. personal computers, laptops and electronic communication devices) at the time of disposal.

In view of such risks, the EDPS emphasised the importance of adopting appropriate **security measures** at every stage of the processing of personal data, including during the phase of disposal of devices containing personal data (from beginning to end).

Moreover, the principle of '**Privacy by Design**' and, in this area, '**security by design**' should be properly taken into account and included in the proposal to ensure that privacy and security safeguards are integrated by default into the design of electrical and electronic equipment.

Personal data stored in electronic waste should be adequately protected.

3.5.5. European Network and Information Security Agency (ENISA)

In an opinion published in December 2010, the EDPS welcomed the extension of ENISA's mandate and the expansion of its current tasks as proposed by the European Commission and underlined that the **security of data** processing is a **crucial element of data protection**. In this respect, he supported the proposal's objective of strengthening the competences of the agency by incorporating **data protection authorities** and **law enforcement bodies** as **fully fledged stakeholders**.

The EDPS recommended more precision with regard to the expansion of the agency´s tasks to avoid legal uncertainty and the need to establish solid cooperation channels with the agency´s stakeholders so that consistency and close cooperation were ensured.

The EDPS also stressed the need to incorporate **security recommendations and best practices** in the internal operations of the Agency. This will allow ENISA better testing and promotion of these techniques in other bodies and agencies.

ENISA´s new Regulation will extend its mandate for five years and will strengthen its competences.

3.5.6. e-Justice

The EDPS is collaborating closely with the Commission and Council teams involved in the inception and operation of the e-Justice action plan. This initiative is intended to modernise and streamline the way people receive legal information so that they can benefit from a 'one-stop multilingual cyber-shop for justice information'.

The site was launched in July 2009 with limited functionality and is intended to incorporate more services following the ambitious roadmap set by the Council that includes among other functionalities: information services, e-Payment, a European order for payment procedure, small claims, search for practitioners and search information in interconnected public registries.

As some of these services are likely to process significant amounts of personal data, the EDPS has recommended, from the outset, the inclusion of appropriate **data protection safeguards** in the legal instruments providing the legal basis and in the IT infrastructure providing the services.

3.5.7. Seventh Framework programme for RTD, including Turbine project

Applying the possible options of interactions listed in his policy paper of April 2008 'The EDPS and EU Research and Technological Development'([10]) the EDPS facilitated contacts and cooperation between national data protection authorities and research project consortiums in 2010.

The case of TURBINE([11])

In 2008, after having analysed the elements of the EU project 'TrUsted Revocable Biometric IdeNtitiEs' (Turbine) which aims at conducting research in the field of **revocable biometrics**, the EDPS decided to reply favourably to a consortium request to produce an opinion on the EU project([12]). The EDPS welcomed the strong relevance of the project to data protection issues and considered that it reflected the priorities identified in his annual report.

Between May and October 2010, the project consortium provided the EDPS with all relevant documents on the data protection aspects of the research conducted in the Turbine project. The EDPS also held several discussions with representatives of the consortium in order to obtain further clarification, and where required, further documents. The demonstrators developed by Turbine and implemented during summer of 2010 were considered an important element of the analysis.

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

([11]) www.turbine-project.eu

([12]) See Annual Report 2008, p. 70.

The key points of the EDPS opinion were presented during the final conference of the project held in Brussels in January 2011.

The Seventh Framework Programme: the starting point of the privacy by design principle.

3.6. International cooperation and data transfers

3.6.1. Passenger Name Records

In 2010, as in previous years, the processing of Passenger Name Records (PNR) by law enforcement authorities raised data protection issues from a European perspective.

With regard to the **US PNR agreement**, the EDPS reiterated some concerns, previously expressed in his interventions before the Court of Justice and in opinions adopted with the Article 29 Working Party, which have not been satisfactorily addressed in the definitive version of the agreement. In particular, the EDPS stressed that the agreement does not focus on persons presenting a risk, but rather envisages bulk collection of personal data and risk assessment applied to all individuals. The PNR agreement with Australia, on the other hand, raised fewer privacy concerns.

The EDPS also took position on a proposal of the Commission to set out its **external strategy on PNR**. The proposal puts forward the general principles, including a set of data protection standards, on which any PNR agreement with a third country

should be based. In his opinion, the EDPS welcomed the horizontal approach followed by the Commission and strongly supported the objective of achieving a high and harmonised level of data protection applicable to all existing and foreseeable PNR schemes.

However, to be acceptable, the conditions for the collection and processing of PNR data should be **considerably restricted.** As with the US PNR agreement, the EDPS was particularly concerned about the **use of PNR schemes for risk assessment or profiling.** He expressed major concerns with respect to the **necessity and legitimacy** of some important aspects of the proposed schemes. In his view, proactive use of the PNR data of all passengers for risk assessment purposes requires more explicit justification and safeguards.

As regards the content of proposed data protection standards, the EDPS called for more precision with regard to the **minimal safeguards** applicable to all PNR agreements. Stricter conditions should apply in particular to the processing of sensitive data, the conditions of onward transfers and the retention of data. The EDPS also emphasised the need for any PNR agreement to make explicit provision to individuals for **directly enforceable rights**.

Personal data of all passengers are used for risk assessment. This raises serious necessity and proportionality issues.

3.6.2. Terrorist Financing Tracking Programme

The EDPS expressed significant concerns about the European Commission's draft agreement with the United States on the **Terrorist Financing Tracking Programme (TFTP)**. The Agreement allows US authorities to access European-based financial data managed by the Belgian company **SWIFT** in anti-terrorism investigations. Further to the decision of the European Parliament to veto the interim agreement in mid-February, the new draft was intended to address concerns regarding privacy and data protection.

*The EDPS considered that **not enough evidence** had yet been provided **to justify the necessity and the proportionality** of such a privacy-intrusive agreement, which in many ways overlapped pre-existing EU and international instruments in this area.*

The EDPS stressed that the **necessity** of the proposed agreement should be established unambiguously, taking into account other existing, less privacy-invasive instruments (e.g. the agreement on mutual legal assistance between the EU and the US). The EDPS expressed particular concerns about the plan to allow the **transfers of massive amounts of bank data** to the US authorities (bulk transfers).

In addition, the opinion indicated the key elements that required improvement from a data protection perspective, including the following:

- ensuring that **bulk transfers** are replaced with mechanisms allowing financial data to be filtered in the EU, and ensuring that only relevant and necessary data are sent to the US authorities;
- considerably reducing the **storage period** for non-extracted data that authorities have not accessed for terrorism-related investigations;
- entrusting the task of assessing requests by the US treasury to a **public judicial authority** in accordance with the negotiating mandate and the current EU legal framework for data protection;
- ensuring that the **data protection rights** of data subjects are **effectively enforceable**, particularly in US territory;
- enhancing **independent oversight** and **supervision mechanisms**

Some of these points have been addressed by the European Commission, the European Parliament and the Council in the final procedure. A slightly revised agreement entered into force on 1 August 2010.

The EDPS expressed his concerns about the plan to allow the transfers of massive amounts of bank data to the U.S. authorities.

3.6.3. EU-US international agreement on information sharing and protection of personal data

The EDPS contributes to the discussions on the drafting of an international agreement on data protection between the EU and the US. This agreement would provide for **high level safeguards** to be applicable to the exchange of personal data in the field of **police and judicial cooperation in criminal matters**.

Since 2007, the EDPS has closely followed the work of the High Level Contact Group involving EU and US representatives and has actively contributed to the different phases of the preparatory work. He issued an opinion in November 2008 and has taken part in the meetings and public consultation organised by the Commission. With regard to the mandate for negotiations drafted by the Commission, the EDPS supported the inclusion of essential data protection requirements in the draft, such as a clear purpose and scope of application, provisions on enforceable rights for data subjects and independent supervision.

3.6.4. Anti-Counterfeiting Trade Agreement

Throughout 2010, the European Union engaged in negotiations to finalise an international Anti-Counterfeiting Trade Agreement (ACTA). The agreement, which was adopted in December 2010, aimed to strengthen the enforcement of intellectual property rights, also on the Internet.

During the negotiations, which were heavily criticised for their lack of transparency, it surfaced that some provisions of the draft agreement were

The EDPS was particularly concerned about ACTA's purported provisions legitimising large scale monitoring of Internet users.

possibly in violation of individuals' rights to privacy and data protection.

> *The EDPS, who had never been consulted on the issue, was particularly concerned about ACTA's purported provisions legitimising* ***large-scale monitoring of Internet users*** *and by the imposition of obligations on Internet Services Providers to adopt '****three strikes Internet disconnection policies****'*([13]).

To address these concerns, the EDPS adopted an opinion in February 2010 that included the following recommendations:

- **investigate less intrusive means to fight piracy on the Internet**: the EDPS took the view that policies based on the three strikes approach are not necessary to achieve the purpose of enforcing intellectual property rights. He requested that less intrusive solutions be considered or, at least, that the scope of the envisaged monitoring be reduced and targeted *ad hoc* monitoring be considered instead;

- **apply appropriate safeguards to all data transfers in the context of ACTA**: insofar as ACTA involves international exchanges of personal data between authorities and/or private organisations located in the signatory countries, the EDPS called on the EU to implement appropriate safeguards on all data transfers made in the context of ACTA. Such safeguards should take the form of binding agreements between EU senders and third country recipients.

3.7. Taxation and customs

3.7.1. Cooperation in the field of taxation

The first EDPS opinion of 2010 concerned a Commission proposal to enhance administrative cooperation between Member States in the field of taxation. The proposal dealt with indirect taxes but did not include VAT and excise duties which are dealt with in other legal instruments.

([13]) These policies would typically involve disconnection of Internet access after prior warnings for alleged illegal sharing or downloading of copyright protected material.

One of the main purposes of the proposal was to improve the exchange of information between Member States. In most cases it concerned information about natural persons. The data protection rules were therefore applicable.

In his opinion, published in January 2010, the EDPS stated that the Commission proposal was a clear example of a **lack of data protection awareness** since the issue of data protection had been almost completely ignored. As a consequence, the proposal contained several elements which were not compliant with data protection requirements. In the opinion these shortcomings were highlighted and discussed.

Amongst other remarks, the EDPS called upon the legislator to define more clearly the responsibility of the Commission for the **maintenance and security of the network** which was intended to be used to exchange information. He also asked the legislator to specify the kind of personal information that could be exchanged, to better define the purposes for which personal data could be exchanged and to assess the necessity of transfers, or at least ensure that the necessity principle would be respected.

3.7.2. EU-Japan joint customs cooperation

In February 2010, the Commission adopted a proposal for a Council Decision on a Union position within the EU-Japan Joint Customs Cooperation Committee concerning the mutual recognition of Authorised Economic Operator Programmes in the European Union and in Japan([14]). Article IV of the Annex of the proposal is related to **information exchange and communication**. The Annex makes provision for information and related data, notably on members of the programmes, to be exchanged in a systematic manner by electronic means.

Both Directive 95/46/EC and Regulation (EC) 45/2001 contain analogous rules in Articles 25-26 and 9 respectively, in connection with transborder flows of personal data. The principle established therein implies that **personal data cannot be transferred** from a Member State to a third country**, unless** that third country ensures an **adequate level of protection** (or unless adequate safeguards are adopted, or one of the exceptions provided for would apply).

([14]) COM(2010)55 final.

Despite the draft Explanatory Memorandum of the proposal declaring the Japanese data protection regime to be adequate, the procedure to determine that a third country ensures an adequate level of protection, as determined in the Directive, had not been respected. As a consequence, the declaration made in the draft Explanatory Memorandum was in violation of the Directive.

The EDPS recommended, therefore, deleting the declaration of adequacy of the Japanese regime included in Point 5(1) of the draft Explanatory Memorandum, since this declaration was not compliant with the requirements of Regulation (EC) 45/2001 and Directive 95/46/EC. He further recommended exploring the different possibilities offered by the Regulation and the Directive in order to ensure that the rules on international transfers would be respected.

3.8. Public access, including Court cases

3.8.1. Public access to documents containing personal data

Since the start of his activities, the EDPS has continuously dealt with the sometimes complicated relationship between EU rules on **public access to documents** and EU rules on **data protection**. The EDPS has first done so by providing guidance to EU institutions. In 2005, for example, the EDPS published a Background paper on the matter entitled 'Public access to documents and data protection', which contained guidelines for EU institutions and bodies.

The EDPS also defended his approach as intervening party in the leading Court case on the subject: *Bavarian Lager v. Commission*. In that case someone had asked for public access to the minutes of a Commission meeting, including the names of the participants. Access to those names was refused on the basis of data protection rules. While the General Court agreed with the position advocated by the EDPS, the Court of Justice in appeal, in its judgment of 29 June 2010, overruled the decision of the General Court and gave a different interpretation of the applicable EU rules.

Part of the analysis presented in the Background paper of 2005 is now no longer valid in the light of the Court's judgment. The EDPS has therefore prepared a short additional paper on this subject which was finalised and published in early 2011.

In this additional paper, the EDPS emphasised the need for a **proactive approach** to the matter. In brief, this means that institutions should make clear to data subjects - before or at least at the moment they collect their personal data - the extent to which the processing of such data includes or might include its public disclosure. The EDPS took the position that institutions were obliged to do so as a matter of good practice.

A proactive approach reduces the number of situations in which institutions have to decide upon public disclosure in a request for public access, such as in the *Bavarian Lager* case. The paper advises on how to strike a fair balance, both in proactive and reactive situations.

Several pending Court cases were suspended awaiting the *Bavarian Lager* judgment. All these cases revived after the judgment of the Court in June 2010. The EDPS was an intervener in several of these cases. Where relevant, the EDPS used the opportunity to express his views on the application of the judgment of the Court in *Bavarian Lager* to these other situations. The EDPS has also provided such input in a newly instigated case on the matter.

The *Bavarian Lager* judgment also entailed as a consequence, that the first case lodged against the EDPS before the General Court, was dismissed.

3.8.2. Other Court issues

Another judgment with EDPS involvement was delivered by the Civil Service Tribunal on 15 June 2010 in *Pachtitis v Commission*. One of the issues at stake in the case was the refusal of the Commission to provide the applicant with access to the questions of a placement test in which he had participated. Since the data protection rules were invoked in this respect and the matter raised an interesting question about the scope of the right of access to one's own personal data, the EDPS intervened. He did so on the side of the applicant. The applicant won the case, but the data protection issue was not dealt with. For that reason the EDPS withdrew from the subsequent appeal instigated by the Commission before the General Court.

In July 2010, the Civil Service Tribunal invited the EDPS to intervene in a case which concerned the transfer of medical data between two EU institutions. It was the first time that the EDPS has

been invited by the Court to intervene in a case. The EDPS accepted the invitation and prepared a statement of intervention in which he clarified the applicable provisions of the Data Protection Regulation.

3.9. A variety of other issues

3.9.1. Internal Market Information System

In July 2010, the EDPS addressed a letter to the Internal Market and Services Directorate-General of the Commission (DG MARKT), in which he took stock of what had been achieved and what further progress needed to be made on the issues raised in the Commission Report on the state of data protection in the Internal Market Information System (IMI).

IMI is an online application that allows Member States to cooperate with each other in order to improve the implementation of Internal Market legislation. This also involves the recording and sharing of relevant personal data. IMI, in particular, allows national, regional and local authorities in EU Member States to communicate quickly and easily with their counterparts in other European countries. IMI helps users to find the right authority to contact in another country and communicate with it using pre-translated sets of standard questions and answers. IMI is designed as a flexible system that can be used for many pieces of single market legislation.

The EDPS welcomed the progress made thus far and encouraged the Commission to implement **further safeguards**, using the principles of **Privacy by Design** and to continue cooperating, as necessary, with data protection authorities in Member States. Importantly, the EDPS also called on the Commission to adopt a new legal instrument, preferably under the ordinary legislative procedure, in order to establish a more comprehensive data protection framework for IMI and to provide legal certainty and a higher level of data protection.

As IMI looks into expansion, a strong legal basis and further data protection safeguards are needed.

3.9.2. Security scanners

From body scanner to security scanner, the solution is privacy by design.

In February 2010, a representative of the EDPS visited the security scanner trial implemented at Schiphol airport in the Netherlands. The objective of the visit was to obtain complementary information on the so called 'second generation of systems' which aims at improving data protection and implementing the 'privacy by design' principle.

In July 2010, the EDPS issued comments([15]) on the Communication related to the use of security scanners at airports adopted by the Commission in June([16]).

([15]) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-07-01_Security_scanners_EN.pdf

([16]) Communication COM (2010) 311 final.

In these comments, the EDPS stressed that **consent** should **not** be used to legitimise processing of personal data if there is no legal basis for that processing.

He also underlined that in the case of security scanners, '**Best Available Techniques**' would mean the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing a defined detection threshold in compliance with the EU privacy and data protection framework.

The EDPS will continue to follow closely the legislative and technical development related to security scanners and will provide any appropriate contribution to the further steps the European Commission plans to adopt in 2011.

3.9.3. Deposit Guarantee Schemes

Deposit Guarantee Schemes reimburse deposits to depositors up to a maximum of EUR 100 000 in case a credit institution goes bankrupt. European rules on such schemes have existed since 1994. Shortly after the outbreak of the financial crisis in 2008, this instrument was reinforced. In July 2010, the Commission put forward another proposal to simplify and harmonise the relevant national rules on the matter.

The reimbursement of deposits through such Guarantee Schemes requires the processing of the data of depositors. The data protection rules are, therefore, applicable, as long as these depositors are natural persons. The data are exchanged between a credit institution and a Deposit Guarantee Scheme, but also between Deposit Guarantee Schemes themselves, either within a Member State or between different Member States.

The EDPS issued a brief opinion on this proposal in September 2010, in which he stated that he was generally satisfied with the way in which the data protection aspects were addressed in the proposal. The proposal for instance ensures that the relevant personal data be used only for the purposes for which they have been exchanged, namely the reimbursement of deposits.

The EDPS was particularly pleased to see that data could only be used in an anonymous format for performing so-called 'stress tests'. During the drafting stage of the proposal, the EDPS had in fact questioned the necessity of using personal data for performing such tests.

3.9.4. Citizens' initiative

The citizens' initiative is one of the innovations introduced by the Lisbon Treaty. It enables a minimum of one million citizens who are nationals of a significant number of Member States to invite the Commission to submit a legislative proposal on a subject of their interest. The collection of at least one million statements of support implies the collection of personal data.

In his opinion of April 2010, the EDPS underlined that full respect for data protection rules would considerably contribute to the reliability, strength and success of this important new instrument.

One of the recommendations concerned the obligation for the organiser of an initiative who intends to use an online collection system to request the competent authority for a certification of the security of such a system. As regards the timing of this request, the EDPS suggested obliging organisers to do so *before* beginning the collection of statements of support rather than after collecting them. The EDPS also suggested that the legislator ensure that:

- personal data collected by the organiser cannot be used for any other purpose than the indicated support of the given citizens' initiative;
- data received by the competent authority can only be used for the purpose of verifying the authenticity of statements of support for a given citizens' initiative.

3.9.5. Investigation and prevention of accidents and incidents in civil aviation

The EDPS' opinion focused on the aspects of the proposal which have an impact on the protection of personal data, including the **processing of data from passenger lists, victims, families and witnesses**, during the different stages of investigations and in the context of an exchange of information between investigating authorities.

The EDPS welcomed the fact that data protection aspects had been taken into account in the proposal.

However, considering the **specific context** in which personal data are processed – the investigation of accidents to improve aviation safety - **further safeguards should be provided to ensure the confidentiality of the data**. This should include provisions requiring the deletion or anonymisation of personal data as soon as possible when they are no longer needed for an investigation.

In the view of the EDPS, more stringent safeguards are needed to protect individuals who are directly or indirectly affected by a serious accident or the loss of relatives.

The EDPS recommendations included the following:

- keeping lists of passengers confidential as a matter of principle, while providing a possibility for Member States to decide in specific cases and on legitimate grounds, including the consent of relatives;
- providing for a limited period of storage of personal data;
- submitting the transmission of personal data to third countries on the condition that they provide an adequate level of protection;
- clarifying the role and responsibilities of the European Commission and of the European Aviation Safety Agency in the application of data protection legislation.

3.10. A look into the future

3.10.1. Technology developments

In previous annual reports([17]) the EDPS already highlighted the **growing convergence** between the **'real world'** and the 'Internet/digital world' or **Information Society**. As a consequence, the distinction between the physical and digital worlds has tended to blur. In 2010, this trend accelerated as convergence has been stimulated by new and innovative tools introduced on a larger scale. So far, it has been possible for individuals to live in parallel realities where they were able to segregate their virtual selves from their real-world selves. This is becoming less and less possible and voluntarily or not, the individual is entering a seamless environment encompassing the electronic and the real worlds, but these worlds are still subject to different regulatory frameworks.

This trend has materialised particularly in **social networks** which continue to expand. The world now spends over 110 billion minutes/year using them([18]) and for the first time a social network website became the most visited website in the US,([19]) overtaking search engines.

The following developments have boosted this phenomenon even more:

- **Smart mobile devices**([20]) constitute one of the main pillars of the new bridges between the physical and the digital worlds. They are always on, ubiquitous and able to share, modify and process information in real time. Their processing power is impressive and they tap into the almost unlimited resources that are available 'in the cloud'. They are capable of recording high-definition images and videos, of tagging objects and individuals individually and of linking geographical coordinates to multimedia material containing places, events and people. Users are permanently connected to the network, processing personal data or having their own personal data processed.
- **Face recognition technology** which has so far been limited to well controlled environments is receiving a new boost as it is starting to be used in social networks and on smart phones. The combination of the brute force of millions of social network users ''armed'' with smart mobile devices uploading photos on which they tag faces of individuals dramatically expands the scope of face recognition technology and even contributes to its improvement. This new emerging trend might also allow the creation of unprecedented large biometric databases from social network platforms.

The concept of **augmented reality** supported by platforms such as smart phones will make it possible to introduce additional information online into the reality of an individual. It is already possible to visit a city and obtain additional

([17]) Annual Report 2007 page 56 and Annual Report 2009 page 64.

([18]) http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/#

([19]) http://www.hitwise.com/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/

([20]) http://www.enisa.europa.eu/media/news-pictures/smartphones-video-clip

information on monuments which are 'identified' by a smart mobile device. Associated with face recognition and social networks as described above, it will become technically possible in the near future to take a picture of someone in the street and access detailed information on that individual in real time.

In the future, **wearable technology** will also constitute a bridge which will promote the merging of an individual's physical daily life with digital landscapes which are not necessarily regulated under the same framework. It will connect people's sensitive data (temperature, blood pressure, hearth beat, sugar rate, etc.) to online applications and services.

These seamless and intertwined worlds open unprecedented advantages for citizens, business and governments, but also bring **unprecedented threats** which will need to be appropriately addressed. In particular, **identity theft in the virtual world** will soon have similar consequences as identity theft in the real world. In light of this, the availability of massive amounts of personal data on a network, the lack of attention for personal data breaches (many of which occur without us being aware of them) and the increased availability of commercial, government and social services to which virtual identifications grant access in the online world constitute a potentially dangerous cocktail. Paper-based and traditional identities no longer represent a satisfactory backup or fall back solution when an electronic identity is also compromised because they are both increasingly embedded in each other.

Despite this blurring of the frontiers between the virtual and real worlds, the applicable rules in both worlds are not similar. To take the example of a smart meter: the production, marketing and use of an electrical meter is subject to a range of specific rules protecting the consumer, but as soon as the same meter is connected to the net and starts describing someone's behaviour, thus becoming a smart meter - for instance, by recording and storing what time a person consumes electricity, it would be possible to know whether a person is at home or not - and such rules may no longer apply. The **review of the data protection framework** could be the appropriate moment for addressing these issues. A legal framework must contribute towards implementing the necessary safeguards that citizens expect to find in this new environment, which needs to be considered trustworthy.

3.10.2. Priorities for 2011

In December 2010, the EDPS published his fifth public Inventory as an advisor on proposals for EU legislation, setting his priorities in the field of consultation for the next year. As in previous years, the EDPS intends to give his opinion on all legislative proposals which have a substantive impact on data protection. He may also look at non-legislative measures whenever they raise substantial data protection issues.

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

- *The **Review of the legal framework for data protection,** which will be one of the top priorities of the EDPS in 2011.*
- *The various initiatives relating to the further **implementation of the Stockholm Programme in the area of freedom, security and justice**, such as the setting up of an entry-exit system and the Registered Traveller Programme, the proposed Directive on the use of PNR for law enforcement purposes, and the introduction of a European TFTP. The EDPS will also closely follow the negotiations for agreements on data protection with third countries. Last but not least, the EDPS will actively participate in the review of the Data Retention Directive.*
- ***Initiatives in the area of technology** which are likely to have an impact on privacy and data protection will be closely considered. The EDPS will continue to follow the further implementation of the **Digital Agenda** for Europe.*
- ***All other initiatives** that may significantly affect data protection, such as initiatives in the area of **transport** (e.g. use of body scanners at airports, e-Mobility packages) and large-scale data exchanges that might take place in the **Internal Market Information System**.*

4 COOPERATION

4.1. Article 29 Working Party

The Article 29 Working Party is an 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([21]).

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 since early 2004 and he considers this 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 2010, the Working Party focused its activities on the four main strategic themes identified in its 2010-2011 work programme, notably:

- implementing the 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 2/2010 on **online behavioural advertising** (WP 171);
- Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for **RFID Applications** (WP 175);

([21]) 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 7/2010 on the European Commission Communication on the **global approach to transfers of Passenger Name Record** (PNR) data to third countries (WP 178).

The Working Party and the EDPS cooperated closely on issues relating to the implementation of Directive 95/46/EC and the interpretation of some of its key provisions. The EDPS actively contributed in different areas such as:

- Opinion 1/2010 on the **concepts of 'controller' and 'processor'** (WP 169);
- Opinion 3/2010 on the **principle of accountability** (WP 173);
- Opinion 8/2010 on **applicable law** (WP 179).

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 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.

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

This work programme deals with different questions, with a focus on common or sensitive issues, where the Group can provide added value and make a difference. Several activities, however,

Coordinated supervision of Eurodac is crucial to uphold the rights of vulnerable people such as asylum seekers.

depend on the adoption of the new Eurodac/Dublin Regulations. They will be implemented when it is most appropriate.

The activities of the Group are now organised according to a timeline, which allows for better forward planning. The work for the coming years is divided between activities to be carried out:

- every four years: e.g. a full security audit is to be carried out by the data protection authorities both at national and EU levels. A coordinated preparation of this audit by the Group will allow for increased efficiency and more comparable results;
- every two years: e.g. coordinated inspections. This involves defining and performing coordinated inspections at regular intervals;
- on a yearly basis: shorter fact-finding activities, with a more restricted perimeter than coordinated inspections, will be carried out according to the needs identified by the Group;
- on a permanent basis: this mainly includes follow-up activities which are needed at a structural level, such as follow-ups on legislative and policy developments, on special searches, and on previous recommendations.

Within these categories, several types of activities have been selected and were started in 2010.

The Group held three meetings in Brussels in March, October and December 2010. At the March meeting, the Group re-elected Mr. Peter Hustinx (EDPS) as Chairman and elected Ms. Elizabeth Wallin (from the Swedish data protection authority) as Vice-Chair.

The Group started working on the **preparation of the full security audit**. A subgroup was appointed and initiated the work by identifying the points for attention, such as the drafting of a list of security objectives. They also worked on the challenges posed by the need to provide comparable results. The work will continue in 2011.

A **new coordinated inspection** was launched at the end of 2010. The Group selected the issue of advance deletion of data and discussed a questionnaire and methodology. The results are expected in 2011. The topic of the advance deletion of data was considered important in view of its impact on data quality in Eurodac and the protection of persons who should no longer be reported in the database.

The **interaction with stakeholders** had a very positive start in the December meeting which was attended by representatives of the United Nations High Commissioner for Refugees and the European Council for Refugees and Exiles. The external stakeholders presented their work and priorities and exchanged views with the Group on issues such as the future of the Dublin System, the information to be provided to asylum seekers or the defence of their rights. The stakeholders also explained their objections to the possibility of giving law enforcement access to Eurodac. This exchange of views proved extremely useful and should be repeated on a regular basis.

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.[22]

The CIS Supervision Coordination Group is set up as a platform in which the data protection authorities, responsible for the supervision of CIS in accordance with Regulation (EC) No 766/2008 ([22]) - i.e. EDPS and national data protection authorities - cooperate in line with their responsibilities in order to ensure coordinated supervision of CIS.

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

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; and

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

In 2010, the EDPS convened two meetings of the CIS Supervision Coordination Group (in March 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 December meeting, the Group adopted the Rules of Procedure which will govern its future work with the CIS and discussed possible actions to be taken in the course of 2011-2012 to ensure comprehensive data protection supervision of the System.

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 certain 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 a different part of the same system.

In 2010, the cooperation mainly concerned the CIS. Since the EDPS and the JSA of the CIS share a supervisory role in the same system, it makes sense to coordinate their action as much as possible. In this spirit, the EDPS invited representatives of the JSA to attend the meetings organised concerning the coordinated supervision of the CIS (see Section 4.3).

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 2010, such as the development of a common supervision policy or the 'Prüm-like' agreements (bilateral agreements on data exchange). The WPPJ also worked with the Article 29 Working Party (WP29) to issue a 'joint contribution of the European data protection authorities' represented in these working groups on the EU-US data protection agreement. This illustrated the need for extensive cooperation between the two groups in a context where a distinction between the former first and third pillars is becoming less relevant.

Finally, the WPPJ broached the subject of its own future in light of the developments mentioned above and in view of the growing involvement of the WP29 in areas traditionally dealt with by the WPPJ.

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.

The European Conference of Data Protection Commissioners took place in **Prague on 29-30 April 2010** under the banner 'Weighing up the past, thinking of the future'. The Conference was hosted by the Czech Data Protection Authority.

The conference included sessions dedicated to various issues, including: 1) Internet of Things; ubiquitous monitoring in space and time - with a presentation by the Assistant Supervisor 2) Children in cobwebs on networks 3) Personal data protection at the crossroads - with a presentation by the EDPS 4) Public sector: respected partner or privileged processor?

Not surprisingly, **the future framework for data protection** currently under preparation by the European Commission was a central theme of the discussions. Several resolutions were adopted, in particular on:

- the envisaged agreement between the EU and the U.S. on data protection standards in the area of police and judicial cooperation in criminal matters;
- body scanners;
- the protection of children;
- the future of privacy.

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.

This year, the International Conference of Data Protection Commissioners was organised by the Israeli Data Protection Authority in **Jerusalem on 26-29 November 2010**. Its main theme was labelled as 'Privacy: Generations'.

Several plenary sessions were organised to discuss the following issues:

- Where are we now? The inter-generational shift in privacy perceptions;
- What's on the regulatory agenda: Hear from the regulators;
- Privacy by Design;
- The future of privacy: How privacy norms can inform regulation.

The Conference further elaborated on the perspectives of different generations on privacy and data protection. A major subject of the conference was how laws and self-regulatory mechanisms influence technology and *vice versa*. The emerging use of social networks was also a key focus of the conference.

The EDPS and the Assistant Supervisor gave presentations and chaired different sessions at the Conference.

The closed session of the Commissioners adopted various resolutions, the most important one being a call for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data.

The 33rd International Conference will take place in Mexico in November 2011.

4.7. International organisations (Florence workshop)

The EDPS, in cooperation with the European University Institute, organised the 3rd workshop on Data Protection in International organisations. It was held in Florence on 27-28 May 2010 and attracted participation from prominent international organisations such as the UNHCR, WCO, IOM, ICC and many others. Discussions addressed various challenges faced by international organisations trying to ensure a good level of data protection in sometimes difficult contexts and without a clear legal basis. These organisations which already achieved a good level of data protection underlined the many benefits it can bring to their core activities (e.g. security of data and legitimacy, in particular).

Following the workshop, the EDPS circulated a questionnaire aimed at taking stock of the data protection arrangements (or the lack thereof) in participating international organisations. The emphasis was placed on how to deliver actual and effective data protection rather than on specific legislative arrangements.

Consequently, the questionnaire builds upon work already done in data protection international *fora* on the concept of accountability as a tool to further induce data controllers to reduce the risk of non-compliance by adopting practical mechanisms for effective data protection. This concept is particularly suitable in the context of international organisations, as it is applicable regardless of the legal environment where data are processed.

The replies will serve as a basis for future action in this context. Many participants have expressed a clear wish to see such workshops organised on a regular basis in the future.

5 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 further consolidated, although significant progress has been made in that sense. 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 has become a point of reference for data protection issues at EU level.

The increased visibility of the EDPS at institutional level is of particular relevance 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.

Activities in 2010 continued to aim at the further improvement of the EDPS' communication actions and information tools. A major development in that respect was the introduction of German as a third language, in addition to English and French, in press and communication activities. This is all the more relevant since German has the most native speakers in the EU. The overall aim is therefore to reach out to a wider audience and give the German-language press and German-speaking citizens the possibility to follow the EDPS' activities in their own language.

5.2. Communication 'features'

The EDPS' communication policy has to be shaped according to specific features that are relevant in view of the age, size and remit of the institution. This requires a tailor-made approach using the right tools to target the appropriate audiences, whilst at the same time being adaptable to a number of constraints and requirements.

5.2.1. Key audiences and target groups

Unlike most other EU institutions and bodies, whose communication policies and activities operate on a general level addressing EU citizens as a whole, the EDPS' direct sphere of action is much more distinct. It is primarily focused on EU institutions and bodies, data subjects in general and EU staff in particular, EU political stakeholders, as well as 'data protection colleagues'. As a result, the 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 essentially depends on a more indirect approach, for instance via data protection authorities at national level.

The EDPS however does his part in raising his profile towards the general public, in particular through 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

The EDPS' communication policy also needs to take account of 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 should therefore be adapted accordingly. When it comes to information and communication tools aimed at a diverse audience, a clear and accessible language which avoids unnecessary jargon needs to be used. Constant 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 more appropriate. Different communication styles and language patterns may therefore need to be used to communicate on the same news.

5.3. Media relations

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

5.3.1. Press releases

In 2010, the press service issued 19 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 negotiations on the Anti-Counterfeiting Trade Agreement (ACTA), the EU-US Agreement on the Terrorist Financing Tracking Programme (TFTP), information management in the area of freedom, security and justice, Privacy and Trust in the Information Society, the EU External Strategy on Passenger Name Record, the evaluation process of the Data Retention Directive and the EU Internal Security Strategy. Relevant rulings by the European Court of Justice were also the subject of press releases, such as the 'Bavarian Lager' case and the ruling on the independence of data protection authorities.

Press releases were also circulated on **key activities in the field of supervision**, in particular relating to the adoption of Guidelines on Video Surveillance and on a comprehensive policy in the field of compliance monitoring and enforcement.

Press releases are published on the EDPS' website and in the European Commission's interinstitutional database of press releases (RAPID) in English and French. A German version was introduced in 2010 to reflect the introduction of German as a third language in the EDPS' communication activities. Press releases are distributed to a regularly updated network of journalists and interested parties. The information provided in the press releases usually results in significant media coverage by both the general and specialised press. They are also frequently published on institutional and non-institutional websites ranging, among others, from EU institutions and bodies, to civil liberty groups, academic institutions and information technology companies.

5.3.2. Press interviews

In 2010, the EDPS gave around 20 interviews to journalists from the print, broadcast and electronic media throughout Europe, with a significant number of requests coming from the German, Austrian, Dutch and US 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 radio and television (e.g. Austrian national television, Dutch and Austrian radio).

The interviews covered horizontal themes such as the trend towards a surveillance society and the current and upcoming challenges in the field of privacy and data protection. They also addressed more specific issues that made the headlines in 2010, including the TFTP agreement with the US, the review of the EU legal framework for data protection and privacy concerns with regard to social networking sites and geolocation applications and the use of body-scanners in airports.

5.3.3. Press conferences

A press conference was organised on 15 November 2010 in Brussels on the review of EU rules on data protection and privacy. Peter Hustinx and Giovanni Buttarelli addressed in particular the Commission communication on a strategy to strengthen EU data protection rules that was published in early November 2010. The press conference also provided an opportunity to present the EDPS 2009 Annual Report and outline the main features of the EDPS' activities in 2009 with regard to his supervisory, consultative and cooperative tasks (see Section 5.7.1).

5.3.4. Media enquiries

Media enquiries are received on a regular basis, and usually include requests for the EDPS' comments and requests for clarification or information. In 2010, media attention mainly focused on the issue of online privacy, in particular as regards new online applications, such as geolocation applications, search engines and social networks – an area which ranked first in the number of enquiries. The agreement with the United States on the processing and transfer of financial data in the framework of the Terrorist Financing Tracking Programme (TFTP) was also of special interest to the press.

The other main issues of interest to the media included the review of the EU legal framework for data protection, the Data Retention Directive, the ePrivacy Directive and its provision on data breaches, the EDPS' supervisory activities, including his guidelines on video-surveillance, the issue of data security, biometric data – both in passports and in the Schengen Information System, international transfers of data, including the Commission's adequacy decisions with third countries and the use of body-scanners in airports.

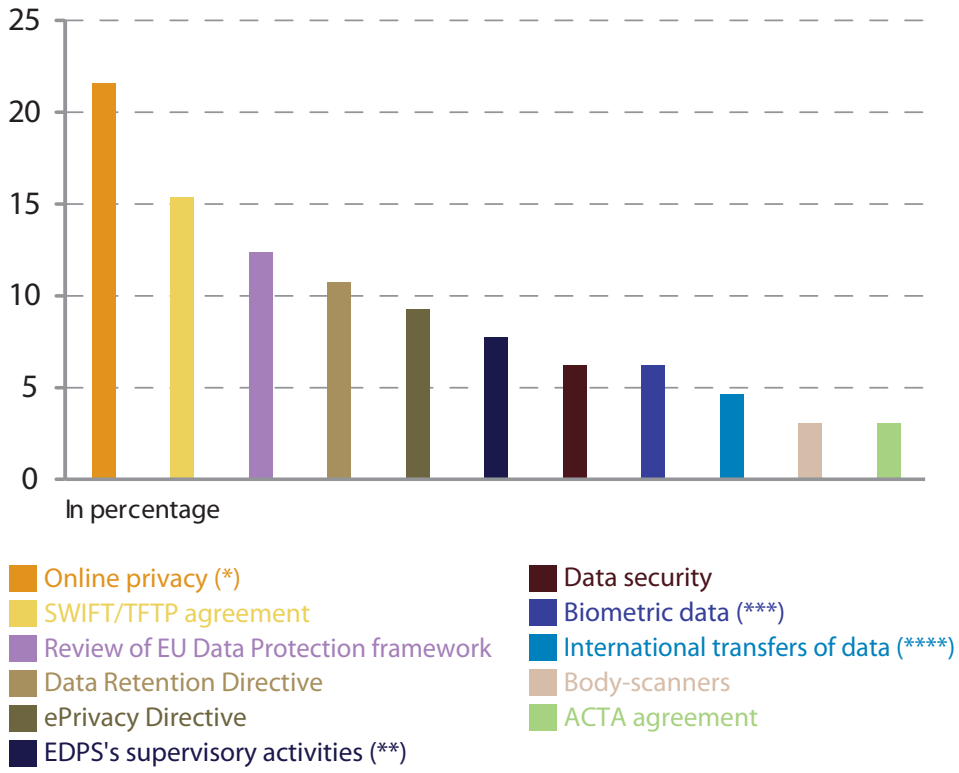
5.4. Requests for information and advice

The number of enquiries for information or assistance received from citizens slightly declined in 2010 (141 requests compared to 174 in 2009). This is mainly due to a decrease in the number of requests dealing with data protection issues at national level and for which the EDPS is not competent. Such an evolution could be seen as a result of the efforts that have been invested in better clarifying the EDPS sphere of competence through his various information and communication tools.

Requests for information come from a wide range of individuals and parties, ranging from

EDPS press conference on the review of the EU legal framework for data protection (Brussels, 15 November 2010)

Main topics for requests from the press in 2010



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

(**) Including video-surveillance guidelines.

(***) Including Schengen Information System.

(****) Including Commission's adequacy decisions.

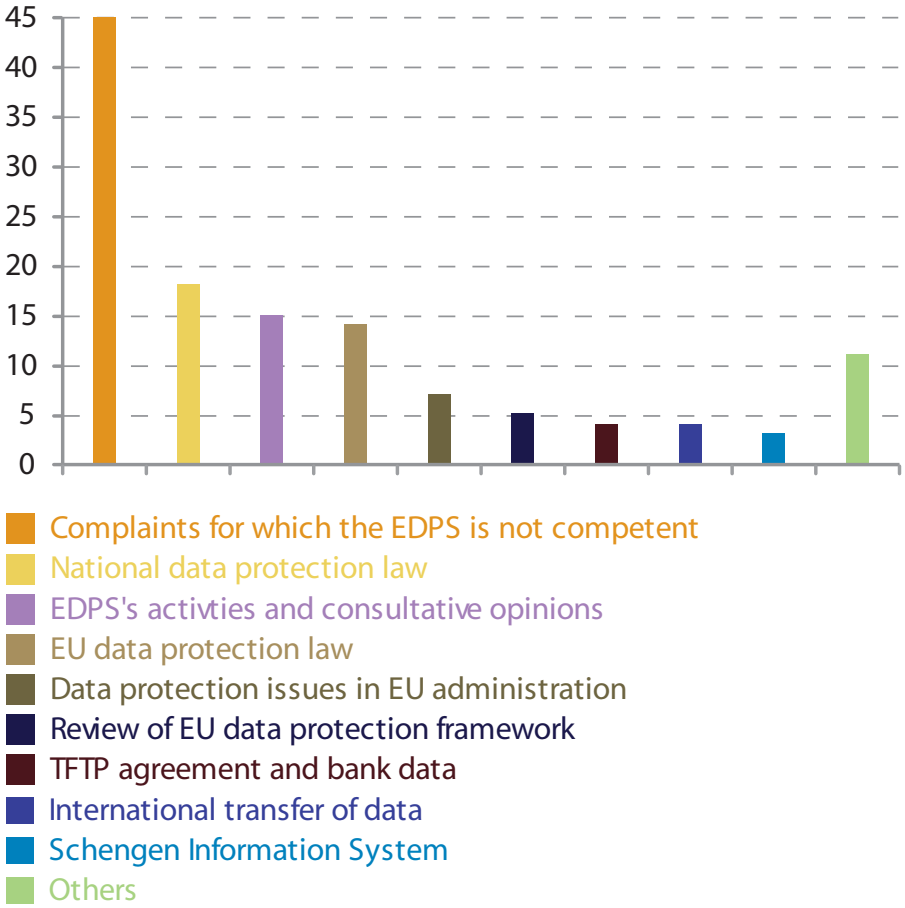
stakeholders operating in the EU environment and/or working in the field of privacy, data protection and information technology (law firms, consultancies, lobbyists, ONGs, associations, universities, etc.) to citizens asking for more information on privacy matters or requiring assistance in dealing with privacy problems they have encountered.

The first category of requests received in 2010 concerns complaints from EU citizens for which the EDPS has no competence. These complaints mostly related to alleged data protection breaches by public authorities, national or private companies and online services and technologies, such as online gaming, blogs, geolocation services, social networking and messaging tools. Others 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. Given that these complaints fall outside the competence of the EDPS, a reply is sent to the complainant specifying the mandate of the EDPS and advising the person to refer to the relevant national authority, usually the data protection authority of the appropriate Member State.

The second category of requests received in 2010, relates to data protection legislation in the EU Member States and/or its implementation at national level. In such cases, the EDPS advises the person to contact the relevant data protection authority and where appropriate, the European Commission's Data Protection Unit.

The remaining categories of information requests mostly fell within the competence of the EDPS and were therefore given substantive replies. They included queries about the EDPS' activities, in particular as regards his work in policy and consultation, about EU data protection legislation, data protection issues in the EU administration, the review of the EU framework for data protection, the TFTP agreement and bank data, international transfer of data and access to the Schengen Information System.

Main areas of information requests from the public in 2010



5.5. Study visits

As part of the efforts to further increase both awareness of data protection and his interaction with the academic world, the EDPS regularly welcomes visits from student groups specialising in the field of European law, data protection and/or IT security issues. In 2010, the EDPS office welcomed seven student groups from several European countries. In October 2010, for instance, the EDPS' office welcomed a group of international and European law students from the Friedrich-Ebert Foundation in Germany to present its role and activities and discuss data protection matters in connection with the Stockholm programme. Other groups of visitors included Austrian MBA students in public management, and students from the University of Tilburg in the Netherlands, from the Rosa Luxemburg Foundation in Germany and from the University of Grenoble in France.

With a view to reaching out to a younger audience, the EDPS' office also welcomed a group of secondary school students from Austria with whom staff members discussed real data protection issues of particular interest to them, such as privacy concerns relating to online social networks.

5.6. Online information tools

5.6.1. Website

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

Web developments

In 2010, the most prominent development brought to the website was the introduction of a German

version, in addition to the existing English and French versions. This initiative is part of the decision to publish all external communication materials in – at least – those three languages in order to better respond to the information needs of both the public and the stakeholders.

The homepage was also reorganised with a view to giving greater prominence to the latest news on the EDPS' activities.

Further improvements to the website are planned and will include:

- the introduction of an online complaint form in order to facilitate the process of submitting complaints and speed-up the processing of complaints by the EDPS' services;
- an overhaul of the prior-check opinions section in order to enhance search possibilities and navigability through thematic categories;
- a streamlined presentation of the notifications register;
- the introduction of a 'press kit' section to provide media professionals with relevant materials and resources that can be used in their news articles and reporting interviews.

Traffic and navigation

As part of ongoing efforts to improve the website performance, many features, some less visible than others, were enhanced in 2009 (e.g. the advanced search tool).

An analysis of the traffic and navigation data shows that, in 2010, the website received a total of 108 215 unique visitors, including more than 12 000 per month in February and March. This represents a fairly significant increase compared to 2009. After the homepage, the most regularly viewed pages were the 'Contact', 'Supervision' and 'Consultation' pages, although the 'News', '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 only used by a very small number of visitors. Such figures lead us to believe that the EDPS' website is consulted by a core of regular visitors who trust its content.

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. 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 on the EDPS' website and a subscription feature is offered on the relevant page.

Five issues of the EDPS newsletter were published in 2010, with an average frequency of one issue every two months. Up to 2010, the newsletter was published in English and French. A German version was introduced in 2010 to reach out to a wider audience and to reflect the use of three working languages in the EDPS' press service.

The number of subscribers rose from 1 200 at the end of 2009 to approximately 1 500 by the end of 2010. 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.

5.6.3. Intranet

With a view to enhancing internal communication and streamlining the exchange of information between the various sectors of the EDPS' office, an Intranet was developed with the assistance of the relevant service of the European Parliament. This new internal portal will be fully operational in early 2011.

5.7. Publications

5.7.1. Annual Report

The annual report is the EDPS' key publication. It provides an overview of the 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.

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

and national level – data subjects in general and EU staff in particular, the EU institutional system, data protection authorities, data protection specialists, interest groups and non-governmental organisations active in the field, journalists and anyone seeking information on the protection of personal data at EU level.

In 2010, a number of improvements, relating both to the form and substance, were made to the report with a view to producing a more reader-friendly publication, while ensuring that the major results and conclusions of the report stand out clearly.

The Supervisor and Assistant Supervisor presented the EDPS 2009 Annual Report to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs on 15 November 2010. The main features of the report were also presented to the press at the press conference organised on the same day on the future of the EU legal framework for data protection (see Section 3.3).

5.7.2. Thematic publications

Preparatory work also started for the publication of thematic 'fact sheets' on data protection issues of strategic importance. The aim will be to provide targeted information guidance to both the general public and interested parties. The first set of fact sheets will cover issues such as the e-Privacy Directive, the SWIFT/TFTP agreement and Passenger Name Record.

EDPS Annual Report 2009

5.8. Awareness-raising events

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

5.8.1. Data Protection Day

The Member States of the Council of Europe and the European institutions and bodies celebrated the fourth European Data Protection Day on 28 January 2010. This date marks the anniversary of the adoption of the Council of Europe's Convention on the protection of personal data (Convention 108), the first legally binding international instrument in the field of data protection.

In past years, the EDPS has used 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 on the premises of the European Parliament, the European Commission, and the Council, in cooperation with the institution's data protection officer. Visitors have the possibility to ask questions to members of the EDPS' office and the data protection officer and test their knowledge of EU data protection in a quiz.

In 2010, the EDPS renewed this specific activity, while investing further efforts in raising awareness among EU staff. A lunchtime debate entitled 'Privacy and data protection: how does it affect you?' was organised at the European Commission on 28 January 2010. Peter Hustinx gave a presentation to Commission staff and answered their questions about data protection rights and the means to exercise them within the EU administration.

A video message from the Supervisor and Assistant Supervisor was also circulated to institutional stakeholders and made available on the website to present the role of the EDPS and outline the challenges ahead.

The EDPS also participated in various events organised in Brussels on the occasion of Data Protection Day, such as the conference and award ceremony that concluded the 'Think privacy' campaign initiated by European Schoolnet and Microsoft. The campaign featured a Europe-wide 'Think Privacy' contest where 15-19 year olds were invited to

Peter Hustinx, EDPS, speaking at the "Think Privacy" conference and award ceremony (Brussels, 28 January 2010)

create and submit a multi-media presentation on the theme 'Privacy is a Human Right – treat it with care'.

On 29-30 January 2010, the EDPS took part in the 'Computers, Privacy and Data Protection' international conference that aims to create a bridge between policymakers, academics, practitioners and activists to discuss emerging issues of privacy, data protection and information technology. For this fourth event, the conference theme was 'An Element of Choice', referring to the many options open for data protection policy. Members of the EDPS' secretariat took part in panel discussions, and Peter Hustinx gave the concluding address at the conference.

5.8.2. EU Open Day

On 8 May 2010, the EDPS office participated, as it does each year now, in the Open Day at the European institutions, organised at the European Parliament in Brussels.

The EU Open Day offers an excellent opportunity to increase general public awareness of the need to protect their privacy and personal information.

The EDPS had a stand in the European Parliament's main building, and staff members from the EDPS' secretariat were present to answer questions from visitors. As with the EDPS' stand for Data Protection Day, information materials were distributed to visitors, together with a quiz on privacy and data protection at EU level.

Visitors filling in a quiz on data protection during EU Open Day.

6 ADMINISTRATION, BUDGET AND STAFF

6.1. Introduction

Ms. Monique Leens, Head of Administration of the EDPS Secretariat since its very inception, retired in June 2010. Her contribution to setting up the EDPS over the last six years was crucial and the EDPS wishes her all the best in her well-deserved retirement. Following her departure, Mr. Christopher Docksey, seconded from the Legal Service of the European Commission on a temporary basis, took over the post of Director of the EDPS *ad interim* and the Secretariat was further strengthened by the recruitment of Mr. Leonardo Cervera Navas, also from the European Commission, as Head of HR, Budget and Administration.

The number of staff substantially increased during 2010. Following the publication of the reserve lists from the general competitions on data protection organised by the EDPS, twelve new officials were recruited. This made it necessary not only to find additional office space but also to adopt a new organisational structure capable of responding to the needs of a larger organisation handling new and complex responsibilities.

The reorganisation of the EDPS, which started with an internal note in April 2010, has continued throughout the year and benefited from the contribution of an external management consultant. This work is expected to continue in 2011 with an extra focus on strategy and performance management.

6.2. Budget

In 2010, a budget of EUR 7 104 351 was allocated to the EDPS by the budgetary authority. This represents an increase of 6.62 % compared to the previous year.

This rise responded to the needs of a bigger organisation with more staff, increased activities and new responsibilities as a result of the entry into force of the Lisbon Treaty. Apart from salaries and building expenses, a significant part of the EDPS budget is allocated to translations due to the fact that EDPS opinions on legislative proposals are translated into all European official languages and published in the *Official Journal of the European Union*. Opinions on prior checks and other published documents are also translated into the working languages of the EDPS (English, French and German).

The Declaration of Assurance (DAS) 2009 of the European Court of Auditors did not call for major changes. The final report contained just two recommendations: the improvement of internal control standards by adopting a system of *ex-post* verification and the creation of a central register to record any exceptions to standard financial procedures.

Assistance from the European Commission in financial matters continued in 2010, particularly in relation to accountancy services, since the Accounting Officer of the Commission is also the Accounting Officer of the EDPS. Within this context, the Commission's Directorate General for

Budget carried out a validation of the local accounting systems procedures and delivered a positive report. The appointment of an Accounting Correspondent was the main recommendation in that report.

All the recommendations in these reports from the European Court of Auditors and the Commission were implemented as follows:

a) a new internal financial verification system has been introduced into the financial workflow;

b) an Accounting Correspondent has been appointed;

c) a central registry of exceptions has been set up; and

d) an *ex-post* verification system is being adopted.

Following the reorganisation of the EDPS, Mr. Christopher Docksey, Director of the EDPS a.i., has been appointed Authorising Officer by delegation and Mr. Leonardo Cervera Navas, Head of HR, Budget and Administration, Authorising Officer by sub-delegation. This new structure gives more flexibility and strengthens the authorisation process of financial transactions of the EDPS.

Where specific rules have not been laid down, the EDPS applies the Commission's internal rules for the implementation of the budget.

6.3. Human resources

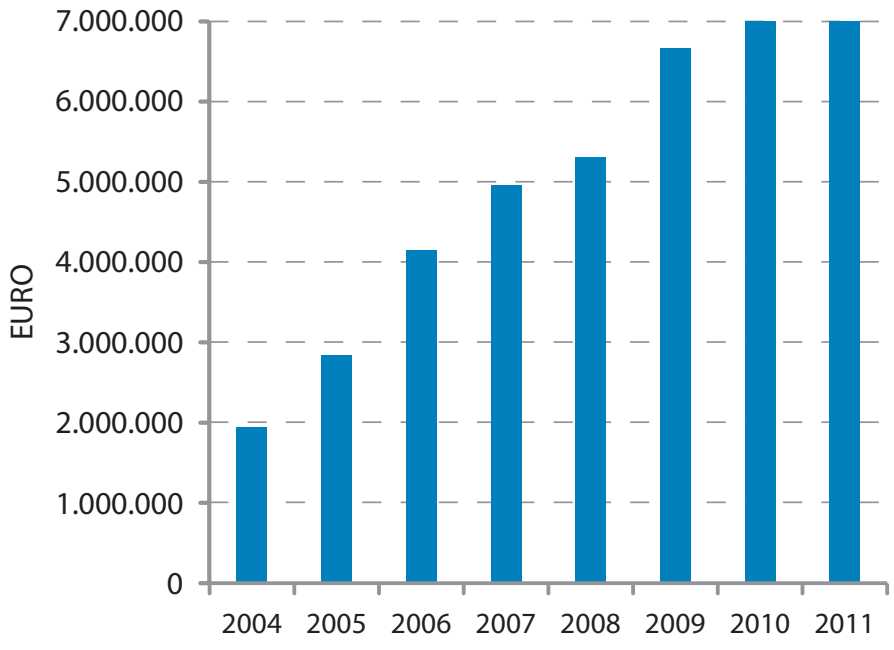
6.3.1. Recruitment

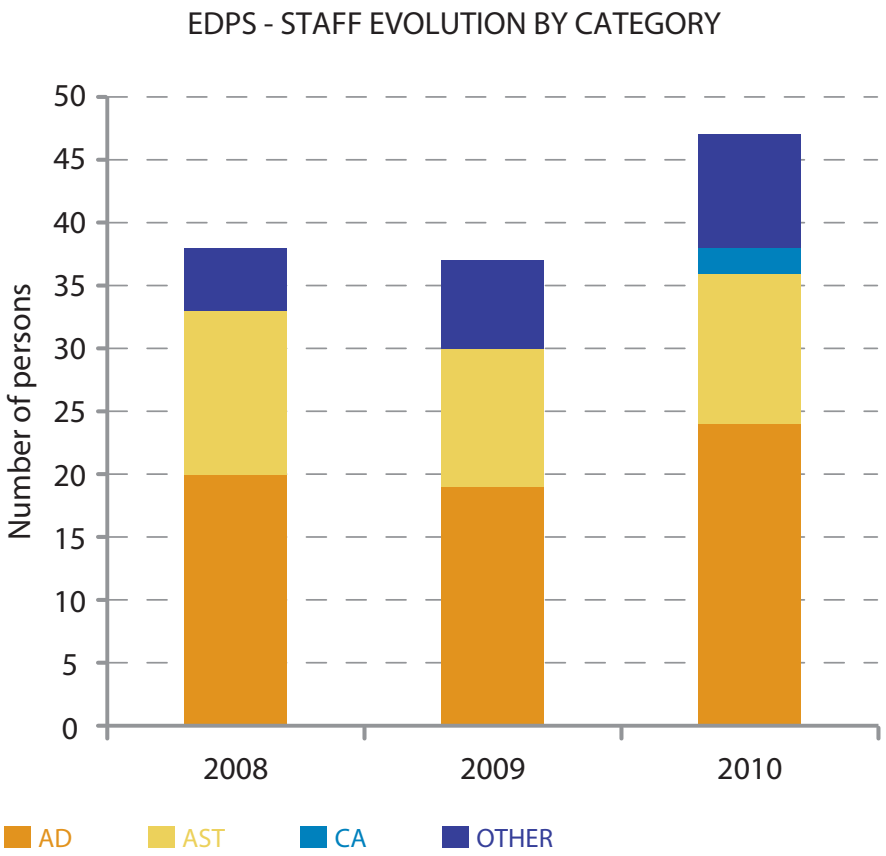
As in previous years and as demonstrated in previous chapters of the present report, the growing visibility of the EDPS is leading to an increased workload and an expansion of tasks which has to be addressed from the human resources perspective.

Thanks to a service level agreement, the EDPS benefits from the services of the European Personnel Selection Office (EPSO) and participates in its board as an observer. As a result, in close cooperation with EPSO, the EDPS launched a general competition on data protection in 2009 so as to recruit highly specialised staff. Three reserve lists were made available in summer 2010 for grades AD9, AD6 and AST3. The validity of the reserve lists has been extended at least until the end of 2011.

Following the publication of these lists, the EDPS embarked on a major recruitment procedure, interviewing candidates from the reserve lists and officials from other institutions, in compliance with Article 29 of the Staff Regulations. During 2010, the EDPS recruited 12 officials and introduced for the first time a new category of staff: contract agents. Further to a selection process of candidates chosen from the CAST lists, two contract agents were also hired. In order to cover temporary needs, an interim secretary was also hired in 2010. Overall, the EDPS recruited 15 new colleagues in 2010.

EDPS - Budget evolution 2004-2011





Finally, the vacancy in the post of Director of the EDPS was published on the interinstitutional recruitment website at the end of 2010. It is expected that this senior recruitment procedure will be completed in the first half of 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 main programme hosts on average two 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 PhD students for non-remunerated traineeships. All the trainees, whether remunerated or not, have contributed to both theoretical and practical work and have also gained 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's Directorate-General for Education and Culture, which has continued to provide valuable support thanks to the extensive experience of its staff.

6.3.3. Programme for seconded national experts

The programme for seconded national experts (SNEs) was launched in January 2006. On average, two national experts from data protection authorities (DPAs) in the Member States have been seconded every year. These secondments have enabled the EDPS to benefit from the skills and experience of such staff and help to increase the visibility of EDPS at national level. At the same time, this programme enables SNEs to familiarise themselves with data protection issues at EU level.

6.3.4. Organisation chart

The EDPS organisation chart remained unchanged since its inception in 2004 up to 2009, when the first reorganisation steps were taken

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 re-organised into five sectors - i.e. Supervision and Enforcement; Policy and Consultation; Registry and Operational Support; Information and Communication; and Human Resources, Budget and Administration - with heads of sector appointed at middle management level. Under the new organisational structure, the Director represents the EDPS at management level and ensures the implementation of policies and horizontal coordination of activities. The Supervisors still retain final responsibility for management, but now concentrate more on policy-making and inter-institutional relations.

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

6.3.5. Training

Providing better training opportunities and career development for staff was one of the priorities for 2010. A new service level agreement was signed with the HR Department of the European Commission which will allow electronic access to the training catalogue of the Commission in early 2011. From then on, the EDPS staff members will benefit from direct access to SYSLOG Formation and will enjoy the same training opportunities as the Commission officials.

Many staff members followed language courses and had access to training organised at interinstitutional level and external training where necessary. The course entitled 'Personal Efficiency Program (PEP)', organised specifically for the EDPS, was particularly successful. This training was attended by three sectors in 2010 and will be attended by all other staff members in the first half of 2011.

Following the EDPS reorganisation, new managers received specific management training and coaching, both as individual managers and as a team.

The EDPS continued to participate in interinstitutional committees (European Administrative School (EAS)'s Interinstitutional Working Party, EAS' Interinstitutional Training Evaluation Group and the Interinstitutional Committee for language training) which facilitates joining forces and allows for economies of scale in an area where needs are essentially similar across the EU institutions. As in previous years, the EDPS signed, together with the other institutions, the protocol on the harmonisation of the cost of the interinstitutional language courses and the new protocol on distribution of costs by institution of pedagogical projects on interinstitutional language.

During 2011, the EDPS will continue efforts to improve the training and career development opportunities of its staff. An update is also planned of the Training Decision of 18 July 2007, in close consultation with the staff.

6.3.6. Social activities

The EDPS has signed a cooperation agreement with the Commission to facilitate the integration of new staff, for instance by providing legal assistance in private matters (rental contracts, buying a house, 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, they also meet members of the HR, Budget and Administration sector who provide them with the EDPS administrative guide and other information on the specific procedures of the EDPS.

The EDPS has continued to develop interinstitutional cooperation with regard to childcare: the children of EDPS staff have access to the *crèches*, after-school childcare and outdoor childcare centres of the Commission, as well as to the European schools. The EDPS is also participating as an observer in the European Parliament's advisory committee on prevention and protection at work, the aim of which is to improve the work environment.

In 2010, the newly created sectors have organised their own away days to foster team spirit and to help newcomers to integrate. A Christmas staff get-to-together was held at the end of the year which provided an opportunity to welcome new colleagues and to take stock of an intensive year full of changes.

6.4. Control functions

6.4.1. Internal control

The internal control system, effective since 2006, ensures that EDPS objectives are met efficiently and in compliance with laws and regulations. The EDPS has adopted specific internal control

procedures according to its needs, its size and its activities. The system has been designed to manage, rather than eliminate the risk of failure to achieve business objectives.

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 it is responsible. Nevertheless, a more ambitious approach was started in 2010. The list of actions that implement the Internal Controls Standards (ICS) has been extended to ensure a more efficient internal control of the processes in place.

By way of example, new case manuals have been adopted to better manage processes such as those involved in prior checking, complaints or court cases. Activities such as awareness-raising actions on ethics, the adoption of more detailed job descriptions, additional internal rules or a new mentoring system are being developed in close consultation with the staff and with the full support of the Supervisors.

6.4.2. Internal audit

The Commission's internal auditor is also the internal auditor of the EDPS. To ensure the effective management of EDPS resources, the internal auditor carries out regular checks of the EDPS internal control systems and financial operations.

Arising from the follow-up audit visit in December 2008 by the Internal Audit Service (IAS), a report adopted in May 2009 confirmed the achievement of the EDPS objectives although it also identified some issues for possible improvement. Some of these issues have already been acted upon and others are being reviewed as the EDPS reorganisation takes place.

A risk assessment exercise by the IAS was scheduled for early 2011 with a view to an audit later in the year.

6.4.3. Security

In December 2010, the EDPS decided to nominate two staff members to the functions of Local Security Officer (LSO), Local Information Security Officer (LISO), and Assistant LSO/LISO respectively on a part-time assignment basis in both cases. First contacts with the European Commission and the European Parliament services have been established and a first area of cooperation has been agreed upon. The process for security clearance of relevant staff has been initiated. Further implementation will focus on information security and information technology (IT) security, in particular relating to the development of the internal Case Management System of the EDPS.

In 2011, the EDPS will continue building on the Security Decision adopted at the end of 2008, which includes measures relating to the management of confidential information and IT security, as well as health and safety conditions for staff and premises.

6.5. Infrastructure

On the basis of the administrative cooperation agreement, the EDPS is located in the premises of the European Parliament, which furthermore assists the EDPS in the fields of IT and infrastructure. In view of the significant increase in the number of staff members in 2010, new office space has been made available with the collaboration of the European Parliament.

The building in which the EDPS is located was partly renovated in 2010. This renovation, carried out under the supervision of the European Parliament, has considerably increased the level of comfort and welfare at work. Nevertheless, space constraints remain a matter of serious concern for the EDPS and the issue has been the subject of several meetings with the European Parliament.

The institution has continued to independently manage its furniture and IT goods inventory, with the assistance of the European Parliament's 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 the 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 2010 (for a two-year period). This cooperation is vital for the EDPS as it increases efficiency and allows for economies of scale.

The inter-institutional cooperation continued in 2010 with various Commission Directorates-General (Personnel and Administration, Budget, Internal Audit Service, Education and Culture), the Paymaster's Office, the European Administrative School (EAS) and various European Parliament services (IT services, particularly with arrangements for the maintenance and development of the 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 agreement with the European Council for translation services came to an end in January 2010. A new agreement was signed with the Translation Centre for the Bodies of the European Union, which has taken over the translation work as of 2010.

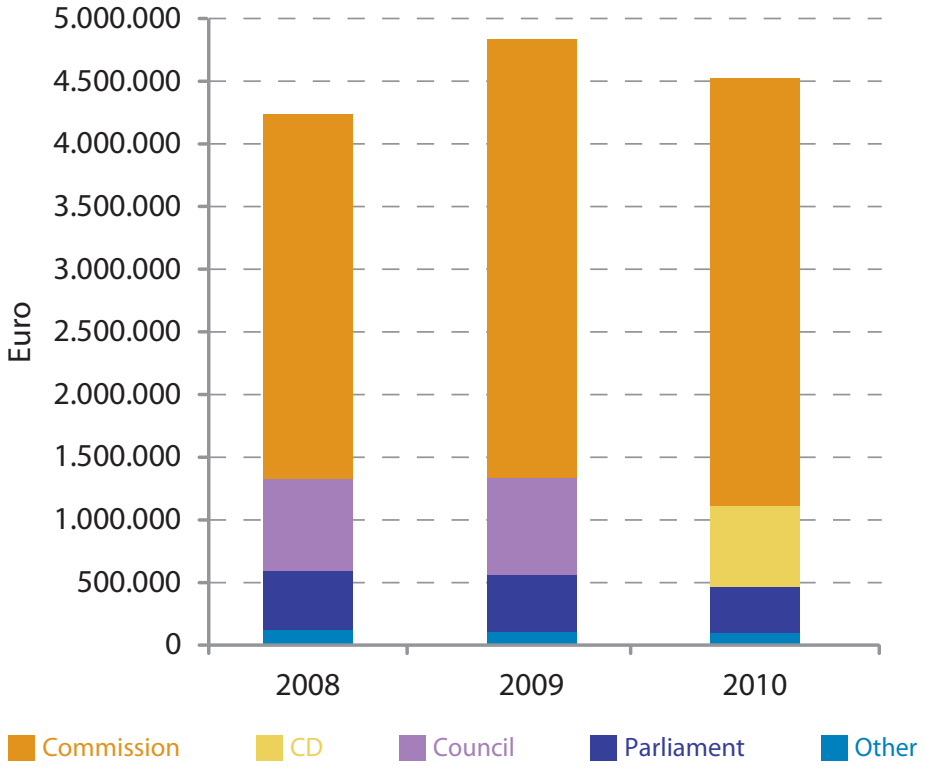
The EDPS is a member of various inter-institutional committees and working groups, including the Collège des Chefs d'administration, *Comité de Gestion Assurances maladies*, *Comité de Préparation pour les Questions Statutaires*, *Comité du Statut*, the Interinstitutional Working Party/EAS, EPSO management board, EPSO working group and *Commission paritaire commune*. The EDPS is a member of the *Comité de préparation pour les affaires sociales* and participates in its *ad hoc* group working on the implementation of the United Nation Convention on the Rights of Persons with Disabilities in the European institutions. This participation helped increase the visibility of the EDPS amongst the other institutions and encourages the sharing of good practices.

6.6.2. Internal rules

The adoption of internal rules for the smooth functioning of the EDPS is an ongoing process. In those areas where the EDPS benefits from the assistance of the Commission or the European Parliament, they are similar to those of the other institutions, albeit with some adjustments to allow for the specific features of the EDPS office.

The EDPS is a relatively young institution and it has been developing fast. As a consequence, the rules and procedures that were suitable during the first years of activity may prove less effective in the

EDPS BUDGET EXECUTION THROUGH INTER-INSTITUTIONAL CO-OPERATION



future, in the framework of a bigger and more complex structure. Rules are therefore subject to ongoing evaluation which may lead to amendments in the coming years. Work was initiated in 2010 with a view to amending the Code of good conduct of the EDPS.

6.6.3. Document management

With the support of the European Parliament's services, a new email management system (GEDA) was successfully implemented for administrative tasks in 2009. Following this first step, studies have been carried out to source an appropriate document and case management system for the data protection department.

During the course of 2010, a detailed set of business requirements for an appropriate document and records management system incorporating case management for the EDPS was drawn up. External consultants were tasked to carry out a market analysis based on these needs to identify appropriate potential solutions. The European Parliament's DG for Innovation and Technological Support (ITEC) continues to support and partner the EDPS in this process. An internal project team led by the Head of the Registry and Operational Support sector was formed. This multi-disciplinary team includes members representing the five different sectors.

In parallel with these technological developments, the Registry and Operational Support Sector has continued to implement accurate records management. A filing plan for four of the five sectors has been adopted and mail registration procedures have been streamlined taking account of the new organisational structure of the EDPS. Particular attention has also been paid to the reporting requirements of the EDPS management. Specific case-related information has been identified and gathered by all sectors to improve case tracking.

7 EDPS' DATA PROTECTION OFFICER

7.1. A new DPO team at the EDPS

As with all other European institutions, the EDPS is subject to specific legal obligations concerning the protection of personal data. These obligations are laid down in the Data Protection Regulation (Regulation (EC) No 45/2001).

Apart from specifying the legal principles governing the processing of personal data by the EU administration, the Regulation provides that each European institution or body must appoint at least one person as a Data Protection Officer (DPO).

In September 2010, the EDPS appointed a **new DPO** and also decided to appoint an **Assistant DPO**. With these appointments the EDPS is investing new energies in this area, to move quickly towards better levels of compliance.

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.

7.2. Action Plan and Implementing Rules

The newly-appointed DPO team circulated to the staff, a comprehensive **Action Plan** with priorities. The Action Plan underlines four main areas where the DPO team intends to put great emphasis: organisational aspects, advisory function, information and raising awareness.

A first important step was the adoption of the **DPO implementing rules** in October 2010. These rules build on other institutions' implementing rules and on the EDPS guidelines, while adapting to the specifics of the EDPS. For example, the guarantee that the DPO may be dismissed only with the consent of the EDPS has been adapted to require the consent of both the Supervisor and the Assistant Supervisor. Furthermore, drawing on the Paper on DPO standards, the implementing rules highlight the need for a sound knowledge of data protection, as well as independence in the reporting process.

7.3. An easily accessible Register of processing operations

The DPO team carried out a thorough check of the **inventory of existing processing operations** and raised awareness among the staff in order to ensure that all processing operations at the EDPS are notified. To this end, controllers were encouraged to prepare missing notifications. The DPO team also provided, where needed, assistance to prepare new notifications and to complete pending ones.

An electronic version of the Register of processing operations has been made available online. This electronic version contains a hyperlink to all final notifications, thus allowing easy access to any person wishing to consult the register, pursuant to Article 26 of the Data Protection Regulation.

The DPO team also updated and improved notification forms that shall be used to notify processing of personal data within the EDPS secretariat.

7.4. Spring exercise

The DPO team followed up the latest 'Spring exercise' (see Section 2.5.2), providing the EDPS with up-to-date information relating to data protection compliance within the institution. The letter sent to the EDPS at the beginning of 2011, highlighted the results achieved and stressed the intention, on the basis of the DPO Action Plan, to step up compliance and awareness about data protection, in particular in the Human Resources area.

7.5. Information and raising awareness

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

With regard to **external communication**, a DPO section, which provides basic information about the DPO role and activities, is now available on the EDPS website. Both the Implementing Rules and the EDPS Register of processing operations are also available online.

In addition, the DPO team has taken part in the **DPO network's meetings**, which represent a unique opportunity to network, discuss common problems and share best practices. The DPO team also played an active role in the activities organised in the framework of the Data Protection Day.

With regard to **internal communication**, the recently established Intranet represents a great opportunity to communicate with staff. The DPO Intranet section contains information that will be useful to staff members: the main elements of the role of the DPO, the implementing rules, the DPO Action Plan and information on the DPO activities. The DPO team also intends to use this virtual space to enhance the visibility of the information that shall be provided to data subjects, pursuant to Articles 11 and 12 of the Regulation. In this regard, the DPO team has started to provide, through the Intranet, references to privacy statements relating to processing operations taking place at the EDPS, with a view to making them easily accessible to all staff.

8 MAIN OBJECTIVES IN 2011

The following objectives have been selected for 2011. The results achieved will be reported next year.

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 continue to invest time and resources in giving advice and guidance on data protection matters. This awareness raising will take the form of guidance papers on selected themes and workshops or interactive seminars whereby the EDPS presents his position in a particular field.

- **Role of prior checking**

Given that the backlog of *ex-post* prior checks has almost been cleared, the EDPS will concentrate on analysing the consequences related to new processing operations. The EDPS will continue to place strong emphasis on the implementation of recommendations in prior check opinions and ensure an adequate follow up.

- **Monitoring and reporting exercises**

The EDPS will continue to monitor the implementation of data protection rules and principles by the institutions and bodies involved, by launching both a general monitoring exercise (Spring 2011) and targeted monitoring exercises where the level of compliance at specific institutions and bodies is a cause for concern.

- **Inspections**

On-the-spot inspections will be launched in those cases where the EDPS has serious grounds to believe that the compliance mechanism is blocked. These will be viewed as the final stage before formal enforcement action. Inspections and audits will also be launched in the field of large-scale IT systems falling within the remit of the EDPS.

8.2. Policy and Consultation

The main objectives are in line with the priorities for this area for 2011, as published on the website. Additionally, objectives have been formulated for cooperation with data protection authorities and for coordinated supervision on large-scale information systems.

- **Scope of consultation**

The EDPS will continue to issue timely opinions or comments on proposals for new legislation and ensure adequate follow-up, in all relevant fields. Special attention will be given, as highlighted below, to the review of the legal framework, the implementation of the Stockholm Programme and initiatives in the area of technology.

- **Review of the legal framework**

The EDPS will give priority to the development of a comprehensive legal framework for data protection. He will issue a legislative opinion on the Commission Communication on a comprehensive approach on personal data protection, as well as on any other ensuing legislative proposals and will contribute to the debate where necessary and appropriate.

- **Implementation of the Stockholm Programme**

The EDPS will continue to give special attention to the various initiatives relating to the further implementation of the Stockholm Programme in the areas of freedom, security and justice, such as the setting up of an entry-exit system and the Registered Traveller Programme, the anticipated Directive on the use of PNR for law enforcement purposes and the introduction of a European TFTP.

- **Initiatives in the area of technology**

Initiatives in the area of technology which are likely to have an impact on privacy and data protection will also be closely considered by the EDPS in 2011. In particular the EDPS will continue monitoring the implementation of the information technology components of Europe 2020 foreseen under the Digital Agenda, such as RFID, cloud computing, eGovernment and online enforcement of intellectual property rights.

- **Other initiatives**

The EDPS will focus on all other initiatives that may significantly affect data protection, such as initiatives in the area of transport (e.g. use of body scanners at airports, e-Mobility package) and large-scale data exchanges that might take place in the Internal Market Information system.

- **Cooperation with data protection authorities**

The EDPS will continue to contribute actively to the activities and success of the Article 29 Data Protection Working Party: influencing its work programme in line with the EDPS priorities, ensuring consistency and synergies between the Working Party and the positions of the EDPS, and maintaining constructive relationships with national data protection authorities. As rapporteur for specific files, the EDPS will steer and prepare the adoption of the WP29 opinions concerned.

- **Coordinated supervision**

Coordinated supervision is required by EU law for Eurodac, the Customs Information System and from mid 2011, the Visa Information System. An important objective for the EDPS will be to provide the data protection authorities involved in coordinated supervision with an efficient secretariat. As supervisor for large-scale IT systems, the EDPS will also participate actively in their coordinated supervision and carry out regular security audits.

8.3. 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 prepare the ground for a review of his Communication Strategy, in particular through a consultation of the main stakeholders. This general exercise will be supplemented by more targeted assessments of the impact of main information and communication tools.

- **Internal organisation**

The main objectives for 2011 will be the completion of the internal reorganisation, renewed efforts on performance management within the context of a strategic review and the development and implementation of new IT tools. Particular focus will also be given to internal control and procedures, better allocation of resources and improved budget implementation.

- **Resource management**

The EDPS will continue investing resources in the development and implementation of a case management system. Priority will also be given to the completion of Service Level Agreements with the European Commission for the deployment of IT applications in the field of human resources (e.g. Syslog Formation, Sysper and Mission Processing Systems).

Annex A — Legal framework

Article 286 of the EC Treaty, adopted in 1997 as part of the Treaty of Amsterdam, provided that Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data also applied to the Community institutions and bodies, and that an independent supervisory authority should be established.

The Community acts referred to in this provision are Directive 95/46/EC, which lays down a general framework for data protection law in the Member States, and Directive 97/66/EC, a sector specific directive which has been replaced by Directive 2002/58/EC on privacy and electronic communications. Both directives can be considered as outcome of a legal development which started in the early 1970s in the Council of Europe (see further below).

On the basis of Article 286 TEC, the European Data Protection Supervisor has been 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, which entered into force in 2001 ([23]). This Regulation also laid down appropriate rules for the institutions and bodies in line with the two Directives.

Since the entry into force of the Lisbon Treaty, the above mentioned Article 286 has been replaced by Article 16 of the Treaty on the Functioning of the European Union, which 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 - now binding - provide that compliance with data protection rules should be subject to control by an independent authority.

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 only being allowed 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, which entered into force on 1 December 2009, 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 its Article 3(1) it applies to the 'processing of personal data by Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which are within the scope of Community law'. However, since the entry into force of the Lisbon Treaty and the abolition of the pillar structure – as a result of which references to 'Community institutions' and 'Community law' have become outdated – the Regulation in principle covers all EU institutions and bodies, except to the extent that other EU acts specifically provide otherwise. The precise implications of these changes 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

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

could be said that Regulation (EC) No 45/2001 is the implementation of that directive at European level. This means that the Regulation deals with general principles like fair and lawful processing, proportionality and compatible use, special categories of sensitive data, information to be given to the data subject, rights of the data subject, obligations of controllers — addressing special circumstances at EU level where appropriate — and with supervision, enforcement and remedies. A separate chapter deals with the protection of personal data and privacy in the context of internal telecommunication networks. This chapter is the implementation at European level of the former Directive 97/66/EC on privacy and communications.

An interesting feature of the Regulation is the obligation for EU institutions and bodies to appoint at least one person as Data Protection Officer (DPO). These officers have the task of ensuring the internal application of the provisions of the Regulation, including the proper notification of processing operations, in an independent manner. All institutions and most bodies now have these officers, and in some cases already for many years. 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
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
ECA	Court of Auditors
ECB	European Central Bank
ECDC	European Centre for Disease Prevention and Control
ECJ	European Court of Justice
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
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

R&D	Research and development
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
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)	Pierre VERNHES	Data.Protection@consilium.europa.eu
European Commission (EC)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Court of Justice of the European Communities (CURIA)	Marc SCHAUSS	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 Ombudsman	Loïc JULIEN	DPO-euro-ombudsman@ombudsman.europa.eu
European Data Protection Supervisor (EDPS)	Alfonso SCIROCCO, Sylvie PICARD (Assistant DPO)	alfonso.scirocco@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)	Benoît VITALE	Data-Protection@cdt.europa.eu
Office for Harmonization 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)	Vincenzo SALVATORE	Data.Protection@emea.europa.eu
Community Plant Variety Office (CPVO)	Véronique DOREAU	Doreau@cpvo.europa.eu
European Training Foundation (ETF)	Liia KAARLOP	Liia.Kaarlop@etf.europa.eu
European Network and Information Security Agency (ENISA)	Emmanuel MAURAGE	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)	Cecile MARTEL	Cecile.Martel@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)	Terry TAYLOR	Taylor@osha.europa.eu
Community Fisheries Control Agency (CFCA)	Clara FERNANDEZ/ Rieke ARNDT	cfca-dpo@cfca.europa.eu
European GNSS Supervisory Authority (GSA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
European Railway Agency (ERA)	Guido STÄRKLE (acting DPO)	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)	Elisabeth ROBINO	Elisabeth.Robino@ecdc.europa.eu
European Environment Agency (EAA)	Gordon McINNES	Gordon.McInnes@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 Chemicals Agency (ECHA)	Alain LEFÈBVRE	Minna.Heikkila@echa.europa.eu
European Research Council Executive Agency (ERCEA)	Donatella PIATTO	Donatella.Piatto@ec.europa.eu
Research Executive Agency (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu

>>>

ORGANISATION	NAME	E-MAIL
Fusion for Energy (The European Joint Undertaking for ITER and the development of Fusion Energy)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu
Sesar Joint Undertaking (SESAR)	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 Institute of Innovation and Technology (EIT)	Camilo SOARES	Camilo.Soares@ext.ec.europa.eu

Annex E — List of prior-check opinions

Empirical analysis of correlations between work system variables and decision-making — OHIM

Opinion of 22 November 2010 on "Empirical analysis of correlations between work system variables and decision-making" notified by the Office for Harmonization in the Internal Market ("OHIM") on 22 July 2010 (case 2010-0468)

Procédures relatives au recrutement d'agents — BEI

Avis du 11 novembre 2010 sur la notification d'un contrôle préalable concernant les procédures relatives au recrutement d'agents (Dossier 2009-0254)

Recruitment procedure and e-Recruitment application tool — EASA

Letter of 19 October 2010 on the notification for prior-checking on a notification for pior-checking concerning "EASA recruitment procedure and e-Recruitment application tool" (Case 2010-0466)

Procedures related to fraud investigations — EIB

Opinion of 14 October 2010 on a notification for Prior Checking on procedures related to fraud investigations in the EIB Group (Case 2009-0459)

Secondment of national experts — CoR

Letter of 5 October 2010 on the notification for prior-checking on secondment of national experts to the Committee of the Regions (Case 2010-0515)

Processing of personal data in frame of deductions from salary in the event of a strike — ECB

Opinion of 28 September 2010 on a notification for Prior Checking on processing of personal data in the frame of deductions from salary in the event of a strike (Case 2009-0514)

Selection and recruitment of staff — EAHC

Letter of 24 September 2010 on the notification for prior-checking on selection and recruitment staff (temporary agents seconded or not from the European Commission, contract agents, interim staff and trainees) at the Executive Agency for Health and Consumers (Case 2010-0346)

Selection of external proofreaders — Commission (Publication Office)

Opinion of 6 September 2010 on the notification for prior checking from the Data Protection Officer of the European Commission concerning "List of participants on examination for proofreaders to work under contract" (Case 2010-400)

Safety Inspections — Commission (DG JRC Ispra)

Opinion of 6 September 2010 on the notification for prior checking from the Data Protection Officer of the European Commission concerning "Safety Inspections at the JRC Ispra Site" (Case 2009-682)

European Surveillance System ("TESSy") — ECDC

Opinion of 3 September 2010 on a notification for Prior Checking on the European Surveillance System ("TESSy") of the European Centre for Disease Prevention and Control ("ECDC") (Case 2009-0474)

Policy on protecting the dignity of the person and preventing psychological harassment and sexual harassment — EASA

Opinion of 29 July on a notification for Prior Checking regarding "EASA policy on protecting the dignity of the person and preventing psychological harassment and sexual harassment" (Case 2010-318)

Implementation of the informal procedure for treating case of psychological and sexual harassment — EESC

Opinion of 28 July 2010 on a notification for prior checking regarding "The implementation of the informal procedure for treating case of psychological and sexual harassment in the Committee" (Case 2010-321)

Selection and recruitment of temporary and contract agents, Seconded National Experts and Trainees — ECHA

Letter of 27 July 2010 on the notification for prior-checking on selection and recruitment of

temporary and contract agents, Seconded National Experts and Trainees (Case 2010-0109)

Processing of personal data in the context of a Quality Process Monitoring — Council

Opinion of 26 July 2010 on a notification for Prior Checking regarding the processing of personal data in the context of a Quality Process Monitoring (Case 2009-0295)

Administrative follow-up of unjustified absences owing to illness — Council

Opinion of 22 July 2010 on the notification of a prior check concerning the dossier "Administrative follow-up of unjustified absences owing to illness" (Case 2009-0687)

Attestation procedure for officials — EMCDDA

Letter of 22 July 2010 on a notification for prior checking concerning the processing activities related to the attestation procedure for EMCDDA officials (Case 2010-0407)

Procedures related to "360° Leadership feedback report" — EIB

Opinion of 20 July 2010 on a notification for Prior Checking concerning procedures related to "360° Leadership feedback report" (Case 2009-0215)

Promotion's procedure for officials and agents — EESC

Opinion of 19 July 2010 on the notification for prior checking regarding the "promotion's procedure for officials and agents" (Case 2008-474)

Selection and recruitment of non-permanent staff — European Investment Bank — EIB

Letter of 14 July 2010 on the notification for prior-checking on the selection and recruitment of non-permanent staff (Case 2009-0678)

Consultation and updating of the central exclusion database — Committee of the Regions

Opinion of 4 June 2010 on the notification of a prior check relating to the file "Procedures to be applied for the consultation and updating of the central exclusion database" (Case 2010-248)

Procedure for dealing with cases of incompetence — Council

Opinion of 4 July 2010 on the notification of a prior check concerning the file "Procedure for dealing with cases of incompetence at the General Secretariat of the Council" (File 2010-237)

Management and Evaluation of external translation carried out by DG TRAD — Parliament

Opinion of 4 June 2010 on the notification for prior checking regarding the "Management and Evaluation of external translation carried out by DG TRAD" (Case 2009-0827)

Temporary employee selection procedure — Commission

Opinion of 4 June 2010 on the notification for prior checking regarding the temporary employee selection procedure (Case 2008-704)

Registration of a Data Subject in the Central Exclusion Database — Commission

Opinion of 26 May 2010 on a notification for prior checking regarding the processing operation on personal data concerning the "Registration of a Data Subject in the Central Exclusion Database" (Case 2009-0681)

Procedure for appointing director-generals, directors and heads of unit — European Parliament

Opinion of 20 May 2010 on a notification for prior checking concerning the procedure for appointing director-generals, directors and heads of unit (Case 2010-0270)

Recruitment of SNEs and trainees — European Centre for Disease Prevention and Control (ECDC)

Letter of 19 May 2010 on the notification for prior-checking on the recruitment of SNEs and trainees (Case 2009-0453)

Recruitment of temporary and contract agents — European Environment Agency (EEA)

Letter of 19 May 2010 on the notification for prior-checking on the recruitment of temporary and contract agents (Case 2009-0467)

Psycho-social and financial support — Joint Research Center (JRC)

Opinion of 10 May 2010 on the notification for prior checking concerning the psycho-social and financial support to the Joint Research Center (JRC ITU) in Karlsruhe (Case 2008-713)

Collection of names and certain other relevant data of returnees for joint return operations — FRONTEX

Opinion of 26 April 2010 on a notification for prior checking concerning the "Collection of names and certain other relevant data of returnees for joint return operations (JRO)" (Case 2009-0281)

Early Warning Response System ("EWRS") — European Commission

Opinion of 26 April 2010 on a notification for prior checking on the Early Warning Response System ("EWRS") (Case 2009-0137)

Internal promotion of official and reclassification of temporary agents — EMCDDA

Opinion of 22 April 2010 on the notification for prior checking regarding the "internal promotion of official and reclassification of temporary agents" (Case 2009-0839)

Processing operations to manage calls for tenders — ETF

Opinion of 22 April 2010 on a notification for prior checking regarding the processing operations to manage calls for tenders (Case 2009-0037)

Dealing with professional incompetence — European Court of Justice

Opinion of 21 April 2010 on the notification of a prior-check on "the procedure for dealing with professional incompetence" (Dossier 2009-860)

Administrative enquiries and disciplinary procedures — EMA

Opinion of 21 April 2010 on a notification for prior checking on the processing of personal data in administrative enquiries and disciplinary procedures (Case 2010-0047)

Procurement procedures and call for expression of interest for selection of experts — Commission

Opinion of 15 April 2010 on the model notification for prior checking concerning "Procurement procedures and Call for expression of interest for selection of experts" (Case 2009-570)

Leadership Effectiveness — Commission

Opinion of 7 April 2010 on a notification for prior checking concerning "Leadership Effectiveness" (Case 2010-0002)

Procédures de sélection du personnel par des panels — BEI

Avis du 26 mars 2010 sur la notification d'un contrôle préalable à propos du dossier "procédures relatives à la sélection du personnel par des panels" (Dossier 2009-679)

Management of leave — Parliament

Opinion of 25 March 2010 on a notification for prior checking on management of leave (Case 2009-595)

Manual filing of disability-related documents of visitors — European Parliament

Opinion of 16 March 2010 on a notification for Prior Checking concerning "Manual filing of disability-related documents of visitors" (Case 2009-564)

Internal mobility procedure — OHIM

Opinion of 15 March 2010 on a notification for prior checking received from the Data Protection Officer of the Office for the Harmonisation of the Internal Market regarding internal mobility (Case 2008-426)

EAS — BELBIN Self perception inventory — European Commission

Opinion of 15 March 2010 on a notification for prior checking received from the Data Protection Officer of the European Commission concerning "EAS - BELBIN Self perception inventory" (Case 2009-377)

Performance appraisal — EMCDDA

Opinion reflected in a letter of 8 March 2010 on a notification of prior checking on the performance appraisal (Case 2009-838)

Management of absences and sickness leave — EESC

Opinion of 5 March 2010 on a notification for prior checking on the management of absences and sickness leave using the "Centurio" database (Joint cases: 2009-0702 and 2009-0703)

Selection of Confidential Counsellors — FRA

Opinion of 10 February 2010 on a notification for prior checking regarding the selection procedures for the selection of Confidential Counsellors (Case 2009-857)

Appointment of middle management staff — Community Plant Variety Office (CPVO)

Opinion of 28 January 2010 on a notification for prior-checking concerning the appointment of middle management staff (Case 2009-0666)

e-Probation — European Investment Bank

Opinion of 21 January 2010 on a notification for prior checking on the processing of personal data in the frame of the management of probationary periods (e-probation) (Case 2009-718)

Complaints by members — Sickness Insurance Management Committee

Opinion of 18 January 2010 on notification of prior checking received from the Sickness Insurance Management Committee in respect of the "Complaints by members" case (Case 2009-070)

Access to private drive and e-mail — Court of Auditors

Opinion of 18 January 2010 on a notification for prior checking regarding the "Procedure to access private drive and e-mail" (Case 2009-620)

Annex F — List of opinions on legislative proposals

European Network and Information Security Agency (ENISA)

Opinion of 20 December 2010 on the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)

EU Internal Security Strategy in Action: Five steps towards a more secure Europe

Opinion of 17 December 2010 on the Communication from the Commission "EU Internal Security Strategy in Action: Five steps towards a more secure Europe"

EURODAC

Opinion of 15 December 2010 on the establishment of 'EURODAC' for the comparison of fingerprints

Proposal for a Regulation on the marketing and use of explosives precursors

Opinion of 15 December 2010 on the proposal for a Regulation on the marketing and use of explosives precursors

EU Counter-Terrorism Policy: main achievements and future challenges

Opinion of 24 November 2010 on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges

Global approach to transfers of Passenger Name Record (PNR) data to third countries

Opinion of 19 October 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries

European Protection Order and European Investigation Order in criminal matters

Opinion of 5 October 2010 on the European Protection Order and European Investigation Order in criminal matters

Information management in the area of freedom, security and justice

Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice"

Deposit Guarantee Schemes

Opinion of 9 September 2010 on the proposal for a Directive of the European Parliament and of the Council on Deposit Guarantee Schemes (recast)

Processing and transfer of Financial Messaging Data from the EU to the US for purposes of the Terrorist Finance Tracking Program (TFTP II)

Opinion of 22 June 2010 on the Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II)

European Agency for the Management of Operational Cooperation at the external Borders (FRONTEX)

Opinion of 17 May 2010 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX)

Sexual abuse of children and child pornography

Opinion of 10 May 2010 on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA

Citizens' initiative

Opinion of 21 April 2010 on the proposal for a Regulation of the European Parliament and of the Council on the citizens' initiative

Waste electrical and electronic equipment (WEEE)

Opinion of 14 April 2010 on the Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE)

Promoting trust in the Information Society

Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy

EU-Japan Joint Customs Cooperation

Opinion of 12 March 2010 on the Proposal for a Council Decision on a Union position within the EU-Japan Joint Customs Cooperation Committee concerning the mutual recognition of Authorised Economic Operator programmes in the European Union and in Japan

Anti-Counterfeiting Trade Agreement (ACTA)

Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)

Accidents and incidents in civil aviation

Opinion of 4 February 2010 on the Proposal for a Regulation of the European Parliament and of the Council on investigation and prevention of accidents and incidents in civil aviation

Cooperation in the field of taxation

Opinion of 6 January 2010 on the proposal for a Council directive on administrative cooperation in the field of taxation

Annex G — Speeches of the Supervisor and Assistant Supervisor

The Supervisor and the Assistant Supervisor continued 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 – Committees

27 January	Assistant Supervisor, LIBE Committee on Counter-terrorism policies (Brussels) (*)
4 March	Supervisor, LIBE Committee on PNR and Transatlantic Privacy (Brussels)
21 June	Supervisor, LIBE Committee on Charter of Fundamental Rights (Brussels) (*)
23 June	Supervisor, LIBE Committee of TFTP II agreement (Brussels)
28 September	Assistant Supervisor, LIBE Committee on combating sexual abuse (Brussels) (*)
9 November	Supervisor, PETI Committee on Public Access to documents (Brussels) (*)
15 November	Supervisor and Assistant Supervisor, LIBE Committee on Annual Report 2009 (Brussels)

European Parliament – Otherwise

28 January	Supervisor, Data Protection Day (Brussels)
9 February	Supervisor, Safer Internet Day (Strasbourg) (*)
16 March	Supervisor, MEPs on ACTA (Brussels)
24 March	Assistant Supervisor, Privacy Platform: Freedom on Internet (Brussels)
8 April	Supervisor, MEPs on PNR (Brussels)
1 December	Supervisor, Privacy Platform: Data Protection Review (Brussels)

Council

19 January	Assistant Supervisor, Conference on ECRIS (Brussels) (*)
25 January	Supervisor, Polish Representation, Data Protection Day (Brussels)
11 February	Supervisor, Conference on Trust in ICT (Leon) (*)
24 March	Supervisor, Working Party on Data Protection (Brussels)

Commission

28 January	Supervisor, Data Protection Day, mini-symposium (Brussels)
28 January	Supervisor, Data Protection Day, lunch speech (Brussels)
22 June	Supervisor, Conference on Intelligent Transport Systems (Brussels) (*)
29 June	Supervisor and Assistant Supervisor, Hearing on Data Protection Review (Brussels)
22 September	Supervisor, Taskforce Social Network Services (Brussels)
5 October	Supervisor, Roundtable on Future of Personal Data Protection (Brussels) (*)
18 November	Supervisor, OLAF Conference (Paris) (*)
3 December	Supervisor, Conference on Data Retention Directive (Brussels) (*)

(*) Text available on EDPS website.

Other EU institutions and bodies

27 January	Assistant Supervisor, Data Protection Day at EMEA (London-Brussels) (*)
7 May	Supervisor, Fundamental Rights Agency (Vienna)
27-28 May	Supervisor and Assistant Supervisor, Workshop International Organisations (Florence)
31 May	Supervisor, Data Protection and Law Enforcement (Trier) (*)
7 June	Assistant Supervisor, EESC on Cyber Harassment (Bratislava) (*)
15-16 June	Supervisor and Assistant Supervisor, Data Protection in Criminal Procedure (Madrid)
13 September	Supervisor, ENISA-FORTH Summer School (Heraklion)
15 November	Supervisor and Assistant Supervisor, Press Conference on AR 2009 (Brussels) (*)

International Conferences

30 January	Supervisor, Computers, Privacy & Data Protection (Brussels)
10 March	Supervisor, Roundtable on 30 years OECD Privacy Guidelines (Paris) (*)
20 April	Supervisor, IAPP Global Privacy Summit (Washington DC) (**)
29 April	Supervisor and Assistant Supervisor, European Data Protection Authorities (Prague) (*)
6 July	Supervisor, Privacy Laws & Business (Cambridge)
25 October	Assistant Supervisor, Public Voice of Civil Society (Jerusalem) (*)
26 October	Supervisor, 30 years OECD Privacy Guidelines (Jerusalem)
27 October	Supervisor, Privacy and Data Protection Commissioners (Jerusalem)
28 October	Assistant Supervisor, Privacy and Data Protection Commissioners (Jerusalem) (*)

Other events

22 January	Assistant Supervisor, 30th anniversary of CRID (Namur) (*)
2 February	Supervisor, European Police Congress (Berlin) (*)
26 February	Supervisor, Intellectual Property and Information Society (Barcelona) (*)
5 March	Supervisor, Colloquium PLN (Brussels)
9 March	Supervisor, British Chamber of Commerce in Belgium (Brussels) (*)
12 March	Assistant Supervisor, Medical Ethics and Patients Rights (San Remo)
23 March	Supervisor, Joint Parliamentary Meeting on Security (Paris) (*)
26 March	Supervisor, Global Mobility and Security (Brussels) (*)
13 April	Supervisor, European Cyber Security Awareness Day (Brussels) (*)
23 April	Supervisor, American Chamber of Commerce in EU (Brussels)
28 April	Assistant Supervisor, Judicial Council (Rome)
11 May	Assistant Supervisor, Workshop on Cloud Computing (Brussels)

(*) Text available on EDPS website.

(**) Video available on EDPS website.

20 May	Supervisor, Data Protection Intensive (London)
1 June	Supervisor, Digital Confidence (Brussels)
2 June	Supervisor, Internet of Things (Brussels)
8 June	Assistant Supervisor, Security Roundtable (Brussels)
15 June	Assistant Supervisor, Lisbon Treaty (London)
17 June	Assistant Supervisor, European Privacy Officers Forum (Brussels)
22 June	Supervisor, American Chamber of Commerce in EU (Brussels)
23 June	Supervisor, Digital EU and IAPP (Brussels)
29 June	Assistant Supervisor, CEPS on Borders and Criminal Justice (Brussels)
8 July	Assistant Supervisor, Alma Graduate School (Bologna)
12 July	Assistant Supervisor, Judicial Council (Rome)
7 September	Supervisor, Future Security (Berlin)
15 September	Supervisor, Privacy and Security (Brussels)
16 September	Supervisor, Lisbon Council on Digital Market (Brussels)
20 September	Supervisor, Counter-terrorism and Data Protection (Brussels)
23 September	Supervisor, Workshop on Data Protection Review (Brussels)
28 September	Supervisor, Data Protection and Freedom of Information (Budapest)
29 September	Supervisor, Information Security and Privacy (Budapest)
29 September	Assistant Supervisor, EU Border Security (Brussels) (*)
13 October	Supervisor, Privacy in a Digital World (Brussels)
22 October	Assistant Supervisor, Criminal Justice in Europe (Luxembourg) (*)
5 November	Assistant Supervisor, Privacy Compliance (Rome)
17 November	Assistant Supervisor, Intelligent Transport (Milan)
23 November	Supervisor, Privacy and Scientific Research (Brussels) (*)
23 November	Assistant Supervisor, Medical Research and Privacy (Brussels) (*)
24 November	Assistant Supervisor, Seminar on Data Protection - video message (Buenos Aires)
29 November	Supervisor, Friends of Europe on EU Data Protection (Brussels)
30 November	Supervisor, Forum Europe on EU Data Protection (Brussels)
30 November	Supervisor, European Internet Forum (Brussels)
2 December	Supervisor, Hogan & Lovells (London)
9 December	Supervisor, Ethics and Governance of Biometrics (Brussels) (*)
10 December	Assistant Supervisor, EU Passengers' Rights (Trier)
16 December	Supervisor, Future Internet Assembly (Ghent) (*)

Annex H — Composition of EDPS Secretariat

The EDPS and Assistant EDPS with most of their staff.

• Supervision and Enforcement

Sophie LOUVEAUX *Head of Supervision and Enforcement*	John-Pierre LAMB *Seconded National Expert*
Laurent BESLAY *Coordinator for Security and Technology*	Xanthi KAPSOSIDERI *Legal Officer*
Jaroslaw LOTARSKI *Coordinator for Complaints*	Luisa PALLA *Supervision and Enforcement Assistant*
Maria Verónica PEREZ ASINARI *Coordinator for Consultations*	Dario ROSSI *Supervision and Enforcement Assistant* *Accounting Correspondent* *External Data Warehouse Manager (EDWM)*

Isabelle CHATELIER *Legal Officer*	Tereza STRUNCOVA *Legal Officer*
Bart DE SCHUITENEER *Technology Officer* *Local Security Officer/LISO*	Michaël VANFLETEREN *Legal Officer*
Delphine HAROU *Legal Officer*	

• Policy and Consultation

Hielke HIJMANS *Head of Policy and Consultation*	Raffaele DI GIOVANNI BEZZI *Policy and Consultation Assistant*
Bénédicte HAVELANGE *Coordinator for Large Scale IT Systems and Border Policy*	Herke KRANENBORG *Legal Officer*
Anne-Christine LACOSTE *Coordinator for cooperation with DPAs*	Roberto LATTANZI *Seconded National Expert*
Rosa BARCELO *Legal Officer*	Alfonso SCIROCCO *Data Protection Officer* *Quality Management*
Zsuzsanna BELENYESSY *Legal Officer*	Luis VELASCO *Technology Officer*
Katarzyna CUADRAT-GRZYBOWSKA *Legal Officer*	

• Registry and Operational Support

Andrea BEACH *Head of Registry and Operational Support*	Kim Thien LÊ *Administrative Assistant*
Christine HUC *Administrative Assistant*	Ewa THOMSON *Administrative Assistant*
Kim DAUPHIN *Administrative Assistant*	

• Information and Communication Sector

Nathalie VANDELLE *Head of Information and Communication*	Agnieszka NYKA *Information and Communication Assistant*
Olivier ROSSIGNOL *Information and Communicant Assistant*	

• Human Resources, Budget and Administration

Leonardo CERVERA NAVAS *Head of Human Resources, Budget and Administration*	Aida PASCU *Administration Assistant* *Assistant LSO*
Isabelle DELATTRE *Finance and Accounting Assistant*	Sylvie PICARD *Assistant Data Protection Officer* *COFO - ICO*
Anne LEVÊCQUE *Human Resources Assistant* *GECO*	Anne-Françoise REYNDERS *Administration Assistant*
Vittorio MASTROJENI *Human Resources Officer*	Marian SANCHEZ LOPEZ *Finance and Accounting Officer*

The European Data Protection Supervisor

Annual Report 2010

Luxembourg: Publications Office of the European Union

2011 — 114 pp. — 21 x 29.7 cm

ISBN 978-92-95073-19-7
doi:10.2804/20023

EUROPEAN DATA
PROTECTION SUPERVISOR

QT-AA-11-001-EN-C

The European guardian of personal data protection

www.edps.europa.eu

Publications Office

ISBN 978-929507319-7