ISSN 1830-5474

Annual Report 2009

European Data Protection Supervisor

Annual Report

2009

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, 2010

ISBN 978-92-95073-07-4
doi:10.2804/10631

Printed in Luxembourg

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

Contents

4 COOPERATION

5 COMMUNICATION

6 ADMINISTRATION, BUDGET AND STAFF

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 2009** presents the main features of the EDPS's work in 2009 and the results achieved in the various fields of activity.

Chapter 2 — **Supervision** describes the work done to ensure and monitor 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 2009. It also presents the thematic guidelines adopted by the EDPS in the fields of recruitment, health data and video-surveillance, as well as an update on the supervision of Eurodac.

Chapter 3 — **Consultation** deals with developments in the EDPS's 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 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, the joint supervisory authorities of the 'third pillar', and the European as well as the international data protection conferences.

Chapter 5 — **Communication** presents the EDPS's information and communication activities and achievements, including external communication with the media and information to the public.

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 — **Main objectives in 2010** provides a brief look ahead and the main priorities for 2010.

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, lists of prior-check opinions and consultative opinions, speeches given by the Supervisor and Assistant Supervisor, and the composition of the EDPS's secretariat.

An executive summary of the present report is also available with a view to providing a concise version of key developments in the EDPS's activities in 2009.

Those who wish to get further details about the EDPS are encouraged to visit our website (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 EU Bookshop (http://www.bookshop.europa.eu) or from the EDPS. Contact details are available on our website, under the 'Contact' section.

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 Community 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

Peter Hustinx, European Data Protection Supervisor, and Giovanni Buttarelli, Assistant Supervisor.

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 with 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 2009 as the fifth full year of activity of the EDPS as a new independent supervisory authority, with the task of 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 the EU institutions and bodies. It also covers the first year of our common five-year mandate as the current two members of this authority.

This year has been of major importance for the fundamental right to data protection. This is due to a few key developments: the entering into force of the Lisbon Treaty, ensuring a strong legal basis for comprehensive data protection in all areas of EU policy; the start of a public consultation on the future of the EU legal framework for data protection; and the adoption of a new five-year policy programme in the area of freedom, security and justice ('Stockholm programme'), with considerable emphasis on data protection as a crucial element for legitimacy and effectiveness in this area.

The EDPS has been strongly involved in these fields 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 is exercised in all regular areas of activity. 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 want 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 that are dealing with the important challenges still ahead.

Finally, we want 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 2009

1.1. Key features

A few developments in 2009 led to increased attention being paid to the fundamental right to the protection of personal data and for up-to-date means to ensure a more effective protection of personal data in practice. This increased attention is very welcome in view of the challenges posed by new technologies, globalisation and conflicting public interests.

The entering into force of the Lisbon Treaty in December 2009 ensured a strong legal basis for comprehensive data protection in all areas of EU policy. The Charter of Fundamental Rights has been given the same legal value as the Treaties. This also applies to its Article 8 on the protection of personal data. Article 16 of the Treaty on the Functioning of the European Union (TFEU) now mentions — among the general provisions of the Treaty — a directly enforceable right for everyone to the protection of his or her personal data.

Article 16 TFEU also provides a general legal basis for legal measures on 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. Compliance with these rules will be subject to the control of independent authorities, as also expressed in Article 8 of the Charter. This will allow — and even require — a complete review of the existing legal framework for data protection, in order to ensure that the full benefits of the fundamental right to data protection are enjoyed by everyone within the scope of EU jurisdiction.

The second key development has been that the European Commission decided to launch a public consultation on the future of the existing EU legal framework for data protection, even before the entering into force of the Lisbon Treaty became a legal and political reality.

This involved a public conference in May 2009 and a public consultation exercise from July until December 2009. The Supervisor and Assistant Supervisor both contributed personally to the conference. They were also very actively involved with their colleagues in the Article 29 Working Party and the Working Party on Police and Justice to ensure a joint contribution to the public consultation, that would allow the Commission to develop a comprehensive legal framework for all areas of EU policy and to ensure its effectiveness in practice, in spite of all the challenges.

The joint contribution of the two working parties, adopted with the full and active support of the European Data Protection Supervisor (EDPS) in December 2009, has been one of the most important contributions to the public consultation. The EDPS will continue to follow this subject very actively in the near future and will be available for further advice as required.

The third key development was the adoption of a new five-year policy programme in the area of freedom, security and justice ('Stockholm programme'),

with considerable emphasis on data protection as a crucial element for legitimacy and effectiveness in this area, shortly after the entering into force of the Lisbon Treaty, also in December 2009. This programme considers the impact of the Lisbon Treaty in this area and sets out the main lines of EU policy in the next five years. Its implementation will in any case also benefit from the institutional changes introduced by the Lisbon Treaty.

The exchange of personal data between migration, law enforcement or public security authorities in the different Member States is an integral part of this policy. Ensuring that data protection is 'built in' in these policies and systems from the start is an important commitment which the EDPS has supported and encouraged actively, and will continue to monitor when and where it is delivered in practice.

These various developments take on even more weight when combined with the start of a new Commission in February 2010, which also puts a considerable emphasis on the protection of fundamental rights in general, and the protection of personal data as a specific subject that deserves high priority. As to the challenges referred to earlier, it is only fair to say that they are to a large extent the consequence of a society that increasingly depends on the widespread use of information technologies in many fields of life.

As this is likely to continue to be the case and become even more relevant in the context of the Commission's Digital Agenda, it should underscore the need for a more effective and comprehensive protection of personal data in the near future. The EDPS is looking forward to the Commission's proposals in all relevant fields and will consider and evaluate them very carefully in due course.

1.2. General overview of 2009

The main activities of the EDPS in 2009 were based on the same overall strategy as before, but continued to grow both in scale and in scope. The capacity of the EDPS to act both effectively and efficiently was also improved.

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

- a 'supervisory' role, to monitor and ensure that EU institutions and bodies ([3]) comply with existing legal safeguards whenever they process personal data;
- a 'consultative' role, to advise EU institutions and bodies on all relevant matters, and 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 2009 are presented. Some key elements will be summarised in this section.

The importance of information and communication about 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 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.

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

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

All EU institutions and bodies must have at least one data protection officer. In 2009, the total number of data protection officers rose to 45. Regular interaction with them and their network is an important condition for effective supervision.

Prior checking of risky processing operations continued to be the main aspect of supervision during 2009. The EDPS adopted 110 prior-check opinions on health data, staff evaluation, recruitment, time management, telephone recording, performance tools and security investigations. 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 'spring 2009' exercise, the EDPS published a report showing that EU institutions have made good progress in meeting their data protection requirements, but a lower level of compliance is observed in most of the agencies.

The EDPS has also carried out four on-the-spot inspections in various institutions and bodies. These inspections are followed up systematically and will be undertaken more frequently in the near future. In July 2009, the EDPS adopted an inspection procedure manual and published the key elements of this procedure on his website.

In 2009, the total number of complaints received rose to 111, but only 42 of these were found admissible. Many inadmissible complaints involved issues at the national level for which the EDPS is not competent. Most issues in admissible complaints involved alleged violations of confidentiality, excessive collection of data, or illegal use of data by the controller. In eight 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 was raised, including transfers of data to third countries or international organisations, processing of data in case of a pandemic procedure, data protection in the Internal Audit Service, and implementing rules of Regulation (EC) No 45/2001.

The EDPS adopted guidelines on the processing of personal data for recruitment and on health data in the workplace. In 2009, the EDPS also held a public consultation on video-surveillance guidelines, among others emphasising 'Privacy by design' and accountability as key principles in this context.

Some EDPS key figures in 2009:

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

➔ **111 complaints received, 42 admissible.** Main types of violations alleged: violation of confidentiality of data, excessive collection of data or illegal use of data by the controller

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

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

➔ **4 on-the-spot inspections carried out** in various EU institutions and bodies

➔ **3 guidelines published** on recruitment, health data and video-surveillance

➔ **16 legislative opinions issued** on large-scale information systems, terrorists' lists, future framework for data protection, public health, taxation and transport

➔ **4 sets of formal comments issued** on public access to documents, universal service and e-privacy and, EU–US negotiations on new SWIFT agreement

➔ **3 Eurodac Supervision Coordination Group meetings organised,** which resulted in a second coordinated inspection report on information to data subjects and assessment of the age of young asylum seekers

Consultation

A number of significant events helped bring the prospect of a new legal framework for data protection closer. Realising this prospect will be a dominant subject on the EDPS agenda in the coming years.

At the end of 2008, a general legal framework for data protection in the area of police and judicial cooperation was adopted at EU level. Although not fully satisfactory, it was an important step in the right direction.

In 2009, a second major development was the adoption of the revised e-privacy directive as part of a larger package. This was also a first step in the modernisation of the legal framework for data protection.

The entry into force of the Lisbon Treaty on 1 December 2009 not only resulted in the Charter of Fundamental Rights becoming binding on institutions and bodies, as well as on Member States when acting in the scope of EU law, but also in the introduction of a general basis for a comprehensive legal framework in Article 16 TFEU.

In 2009, the Commission also launched a public consultation on the future of the legal framework for data protection. The EDPS has worked closely with colleagues in order to ensure an adequate joint input to this consultation and has used various occasions to highlight the need for more comprehensive and more effective data protection in the European Union.

The EDPS continued to implement his general consultation policy and issued a record number of legislative opinions on different subjects. This policy also provides for a proactive 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 Parliament and Council.

In 2009, the EDPS followed with particular interest the developments concerning the Stockholm programme and its vision for the next five years in the area of justice and home affairs. The EDPS advised on the development of the programme and took part in the preparatory work for the European Information Model.

Other work in this area related to the review of the Eurodac and Dublin regulations, the setting up of an agency for the operational management of large-scale IT systems, and a coherent approach to supervision in this field.

In the context of e-privacy and technology, apart from the general review mentioned above, the EDPS was involved in issues relating to the data retention directive, the use of RFID tags or intelligent transport systems, and the RISEPTIS report on 'Trust in the information society'.

In the context of globalisation, the EDPS was involved in the development of global standards, the transatlantic dialogue on data protection and law enforcement data, as well as in issues around restrictive measures with regard to suspected terrorists and certain third countries.

Other areas of substantial EDPS interest have been public health (including cross-border healthcare, e-health and pharmaco-vigilance) and public access to documents, such as the revision of public access Regulation (EC) No 1049/2001 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 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 cooperated well on a range of subjects, but especially on the implementation of the data protection directive and on the challenges raised by new technologies. The EDPS also strongly supported initiatives taken to facilitate international data flows.

Special mention should be made of the joint contribution to the 'future of privacy' in reply to the consultation of the European Commission on the EU legal framework for data protection, and the consultation of the Commission on the impact of 'body scanners' in the field of aviation security.

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 Coor-

dination Group — composed of national data protection authorities and the EDPS — met three times and concentrated on the implementation of the work programme adopted in December 2007.

One of the main results was the adoption in June 2009 of a second inspection report focusing on two issues: the right to information for asylum seekers and the methods for assessing the age of young asylum seekers.

The EDPS continued its close cooperation with data protection authorities in the former 'third pillar' — the area of police and judicial cooperation — and with the Working Party on Police and Justice. This included in 2009 contributions to the debate on the Stockholm programme and evaluating the impact of the Council framework decision on data protection.

Cooperation in other international forums continued to attract attention, especially the 31st International Conference of Data Protection and Privacy Commissioners in Madrid, which led to a set of global standards for data protection.

The EDPS also organised a workshop on 'Responding to security breaches' in the context of the 'London initiative' launched at the 28th International Conference in November 2006 to raise awareness of data protection and to make it more effective.

1.3. Results in 2009

The Annual Report 2008 mentioned that the following main objectives had been selected for 2009. Most of these objectives have been fully or partially realised.

- Support of the DPO network

The EDPS continued to give strong support to data protection officers, particularly in recently established agencies, and encouraged an exchange of expertise and best practices among them, in order to strengthen their effectiveness.

- Role of prior checking

The EDPS nearly completed prior checking of existing processing operations for most institutions and long-standing bodies, and put increasing emphasis on the follow-up of recommendations. Prior checking of common processing operations in agencies received special attention.

- Horizontal guidance

The EDPS published guidelines on staff recruitment and health data at work, and draft guidelines on video-surveillance which were the subject of a consultation. These guidelines are designed to help ensure compliance in institutions and bodies and to streamline prior-checking procedures.

- Complaint handling

The EDPS adopted a manual for staff on the handling of complaints and published its main lines on the website to inform all parties involved about relevant procedures, including criteria on whether or not to open an investigation on complaints presented to the EDPS. A complaint form is now also available on the website.

- Inspection policy

The EDPS continued to measure compliance with Regulation (EC) No 45/2001, with different kinds of checks, for all institutions and bodies, and executed a number of inspections on the spot. A first set of inspection procedures was published to ensure a more predictable process.

- Scope of consultation

The EDPS issued a record number of 16 opinions and four sets of formal comments on proposals for new legislation, on the basis of a systematic inventory of relevant subjects and priorities, and ensured adequate follow-up. All opinions and comments as well as the inventory are available on the website.

- Stockholm programme

The EDPS gave special attention to the preparation of the new five-year policy programme in the area of freedom, security and justice, adopted by the Council at the end of 2009. The need for effective data protection has been recognised as a key condition.

- Information activities

The EDPS improved the quality and effectiveness of the online information tools (website and electronic newsletter) and updated other information activities (new information brochure and awareness-raising events), where necessary.

- Rules of procedure

Rules of procedure for the different activities of the EDPS will be adopted soon. They will mostly confirm or clarify present practices and will be available on the website.

- Resource management

The EDPS consolidated and further developed activities relating to financial and human resources and gave special attention to the recruitment of staff by means of an EPSO competition in data protection. The first successful candidates are expected in the course of 2010.

2

SUPERVISION

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 that either completely or partially fall within the scope of — what used to be — 'Community law' [4] (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 TFEU which replaces Article 286 of the EC Treaty. The precise implications of both this change and the abolition of the pillar structure for the supervision activities of the EDPS are currently being examined and may require further clarification.

Prior checking of processing operations continued to be an important aspect of supervision during 2009 (see Section 2.3), but the EDPS 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.

During 2009, as in previous years, there was no need for the EDPS to use his powers to order, warn or ban, as controllers have implemented the EDPS's recommendations, expressed the intention of doing so or are taking the necessary steps. However, the promptness of the responses differs from one case to another.

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 2009, seven new DPOs were appointed in new agencies or joint undertakings, bringing the total number of DPOs to 45.

For a number of years, the DPOs have met at regular intervals in order to share common experiences and discuss horizontal issues. This informal network has proved to be productive in terms of collaboration and continued during 2009.

A 'DPO quartet' composed of four DPOs (Council, European Parliament, European Commission and Translation Centre for the Bodies of the European

[4] Article 3(2) of Regulation (EC) No 45/2001.

Union) was set up with the goal of coordinating the DPO network. The EDPS collaborated closely with this quartet.

The EDPS attended the DPO meetings held in March 2009 at the European Central Bank and in October 2009 at the European Commission (co-hosted with OLAF), using the opportunity to update the DPOs on EDPS work, give an overview of recent developments in EU data protection and discuss issues of common interest. More specifically, the EDPS used this forum to explain and discuss the procedure for prior checks, to report on progress of prior-checking notifications, to update the DPOs on the 'spring 2009' exercise and its follow-up (see Section 2.5), to give an update of EDPS inspections and to present the EDPS inspection policy and procedure. The EDPS also used this occasion to relaunch work on the setting of professional standards for DPOs and to share initiatives for European Data Protection Day (28 January).

Data protection officers during their 26th meeting in Brussels (October 2009).

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)). For example, the EDPS considers that the presence of some biometric data other than photographs alone presents specific risks to the rights and freedoms of data subjects and justifies the prior checking by the EDPS of the processing activity. These views are mainly based on the nature of biometric data which is inherently sensitive.

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 the previous years ([5]) continued to be applied in the interpretation of this provision, both when 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

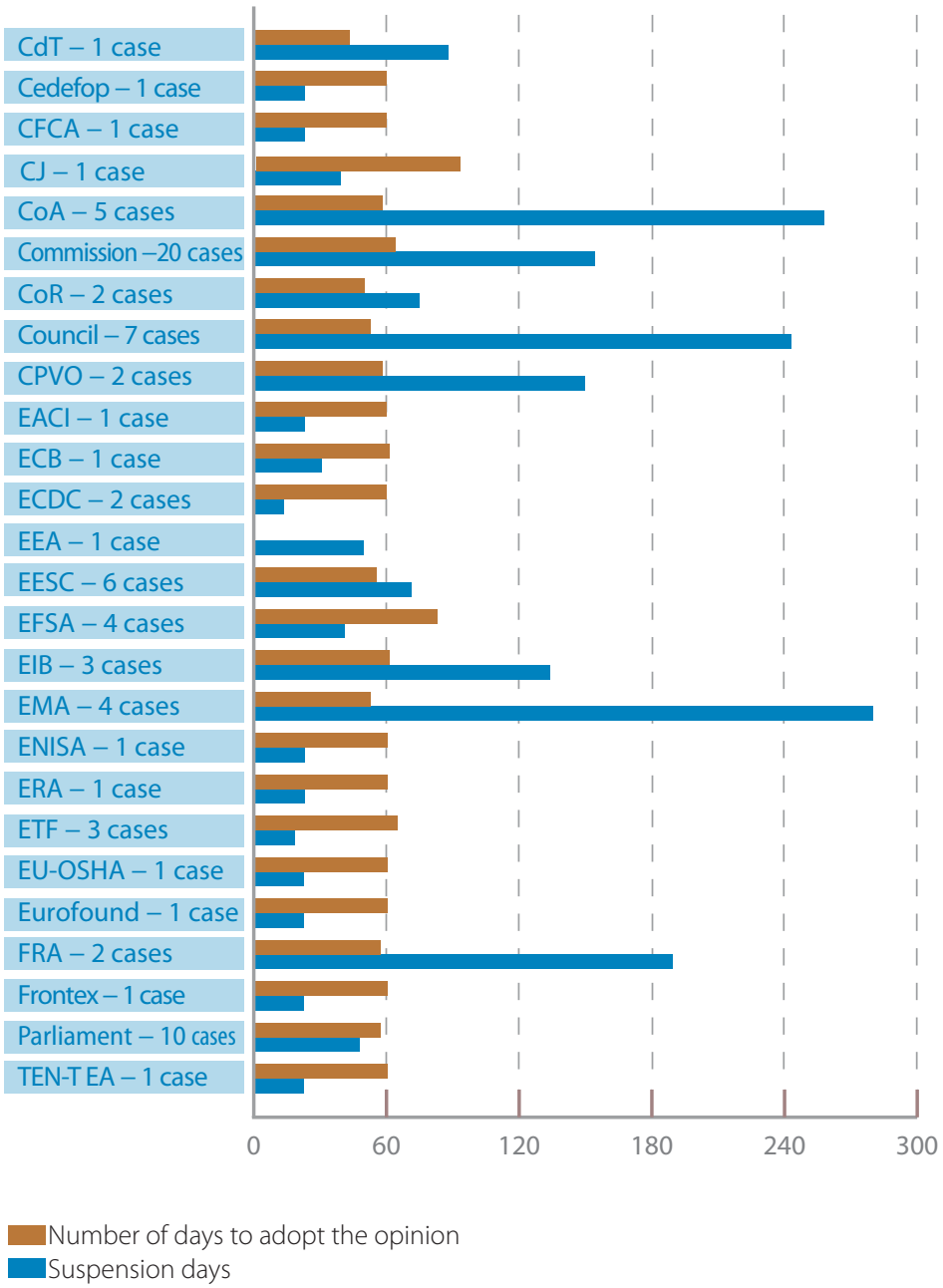
Prior checks must be carried out by the EDPS following receipt of a notification from the DPO. Should the DPO be in doubt as to whether a processing operation should be submitted for prior checking he or she may consult the EDPS (see Section 2.3.4).

Prior checks involve not only operations not yet in progress, but also processing that started before 17 January 2004 (the appointment date of the 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.

([5]) See Annual Report 2005, Section 2.3.1.

Period, suspension and extension

Average deadlines per institution/agency

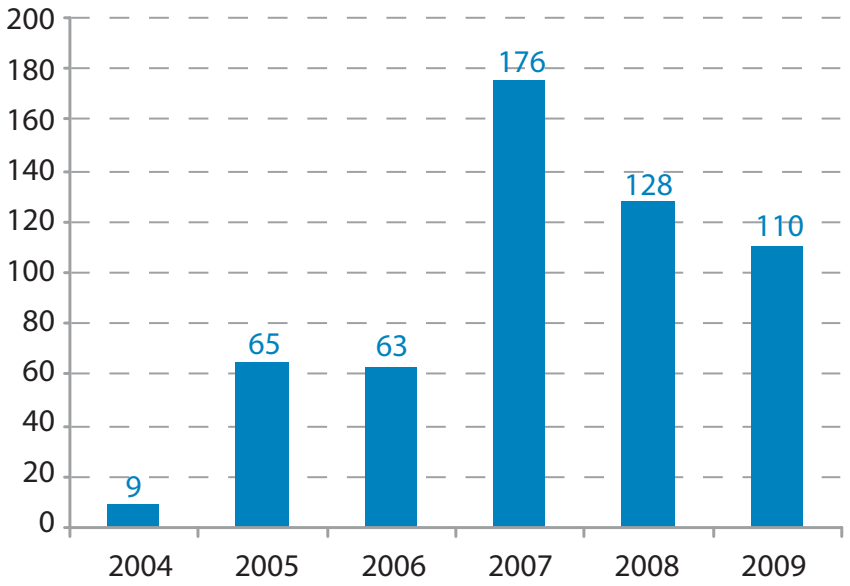


The EDPS must deliver his opinion within two months of receiving the notification ([6]). Should the EDPS make a request for further information, the period of two months is usually suspended until the EDPS has obtained this information. This period of suspension includes the time given to the DPO for comments, and 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.

([6]) For *ex post* cases received before 1 September 2009, the month of August has neither been calculated for institutions and bodies, nor for the EDPS.

Register

Notifications to the EDPS



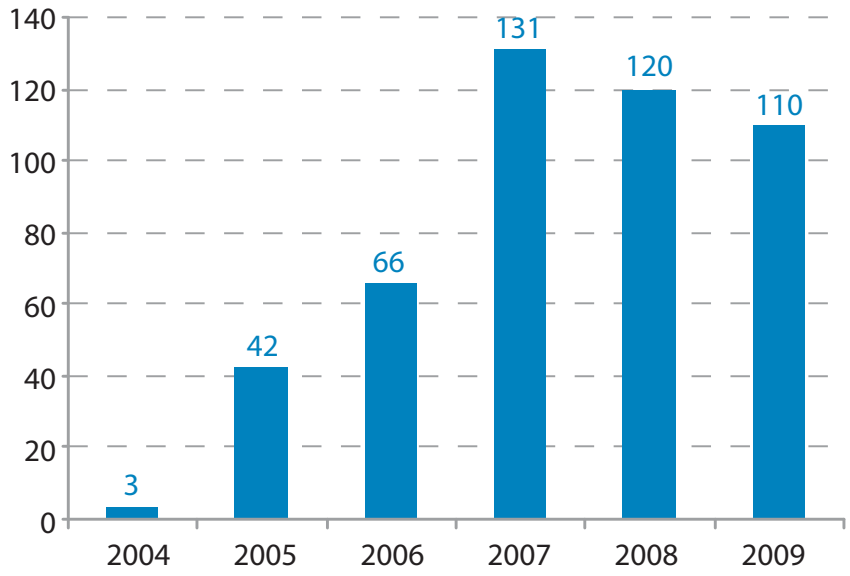
In 2009, the EDPS received 110 notifications for prior checking. This figure shows a slight decrease in comparison to 2008 as the EDPS reaches the end of the backlog of *ex post* prior checks.

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)).

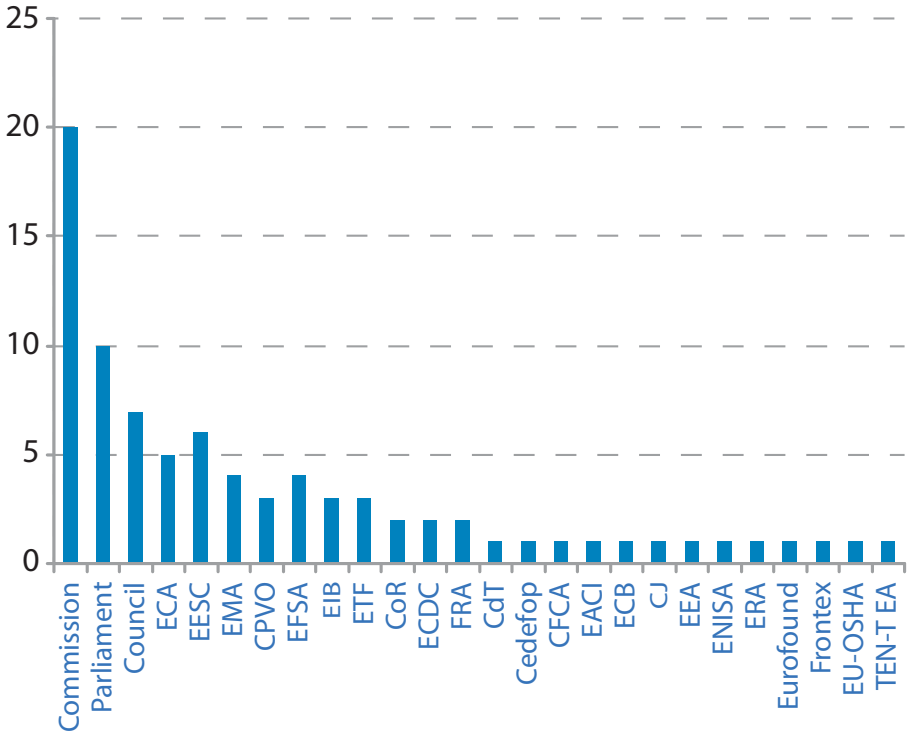
This register must contain the information referred to in Article 25 and be open to public inspection. In the interests of transparency, all information is included in the public register available on the EDPS website (except for the security measures which are not mentioned in the register).

Opinions

EDPS prior-check opinions per year



EDPS prior-check opinions per institution in 2009



The final position of the EDPS takes the form of an opinion, to be notified to the controller of the processing operation and to the DPO of the institution or body (Article 27(4)). **In 2009, the EDPS adopted 110 prior-checking opinions** (see above 'EDPS prior-check opinions per year' chart). This represents a slight decrease compared with the previous two years.

The **larger institutions** represent the **majority of these opinions** with 20 opinions on processing operations at the European Commission, 10 at the European Parliament and 7 at the Council (see above 'EDPS prior-check opinions per institution' chart). Many agencies have also started notifying core business activities and standard administrative procedures according to the relevant procedures established by the EDPS (see Section 2.3.2).

Opinions contain a description of proceedings, a summary of the facts, and a legal analysis examining whether the processing operation complies with the relevant provisions of the regulation. Where necessary, recommendations are made to the controller to the effect of ensuring compliance 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 EDPS's opinions are adopted after a complete analysis of all significant information. It provides a structure for opinions, based on accumulated practical experience and is continuously updated. A workflow system is in place to make sure that all recommendations in a particular case are followed up and, where applicable, that all enforcement decisions are complied with (see Section 2.3.6).

Procedure for *ex post* prior checks in agencies

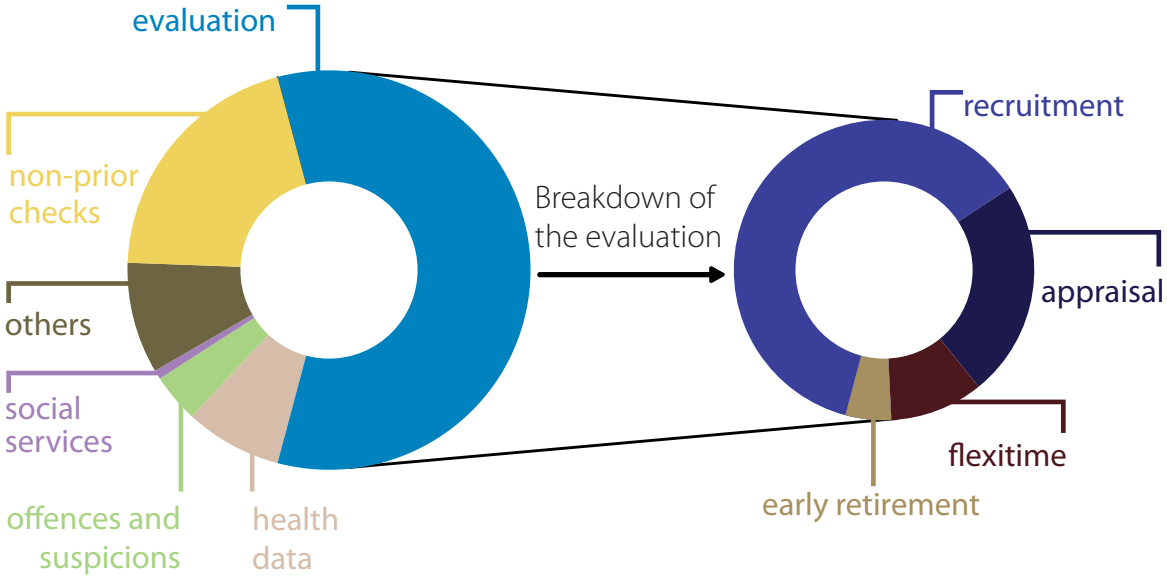
In October 2008, the EDPS launched a new procedure for *ex post* prior checks in the EU agencies. Since in many cases standard procedures are the same in most EU agencies and are based on Commission decisions, the idea is to gather notifications on a similar theme and to adopt either a collective opinion (for various agencies) or a 'mini prior check' addressing only the specificities 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 below, 'Thematic guidelines'). The DPO will then submit an Article 27 notification with a cover note highlighting specific aspects vis-à-vis the position of the EDPS in this field (specificities of the processing within the agency, problematic issues, etc.).

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. The EDPS was still in the process of receiving notifications in this field prior to adoption of a horizontal opinion early 2010.

2.3.3. Main issues in prior checks

Opinion 2009 per category



Medical data and other health-related data

European institutions and agencies process medical data and other health data on individuals in a number of situations related to the application of the Staff Regulations (pre-recruitment medical examination, annual medical examination, reimbursement of medical expenses, medical certificates justifying sick leave, etc.). Due to the particularly sensitive nature of health-related data, processing operations involving such data are subject to prior checking by the EDPS.

In 2009, the EDPS continued to adopt a number of opinions in the field of health data (see chart above).

In September 2009, the EDPS issued guidelines on the processing of such data in view of notifications of processing operations relating to health related data by EU agencies (see Section 2.7 below, 'Thematic guidelines'). These guidelines also serve as a set of EDPS standards for institutions.

The EDPS prior checked a particular case relating to the processing of health-related data by the **security support system** at the European Parliament (Case 2009-225). The collection of data in the security support system is designed to provide support to missions outside the three places of work of the Parliament in case of medical emergencies. The information is provided by the data subject on a voluntary basis and data will only be used in emergency situations and only given to local health staff if needed.

The EDPS conceded that the processing of health-related data could be based on the consent of the data subjects in accordance with Article 5(d) and Article 10§2(a) of the regulation. Although the EDPS underlined that, in the context of employment, the use of 'consent' as a legal basis presents some restrictions, nevertheless, in the case under analysis, the data subject is free to provide the categories of data mentioned above and is informed about the possible consequences of not providing the information.

The processing of personal data by **interinstitutional crèches** in Brussels (Case 2009-088) and in a day nursery and study centre in Luxembourg (Case 2009-089) raised some particular data protection issues relating to medical data. In the case of the processing done by the crèches in Brussels, the EDPS particularly criticised the fact that the processing of medical data goes further than just verifying admissions to the crèches and reacting in emergency cases, and creates *de facto* medical monitoring of the children by the medical service of the Commission.

The EDPS recommended that the monitoring of the health and growth of the children by the crèches or other day-care centres should be done by the medical service only on a voluntary basis with the express consent of the parents.

The EDPS also criticised the 30-year period adopted by the Commission during which it stores the medical files of the children registered with the crèches in Brussels. A similar criticism was addressed to the day nursery and study centre in Luxembourg, where medical data are kept for 10 years and then archived. The EDPS recommended that these retention periods are reviewed according to the specific need for the data and files. The EDPS further recommended that parents have the option to transfer the medical file of their child to their doctor after the child leaves the crèche.

Furthermore, in both cases the EDPS considered it essential that staff working at the crèches/day nursery/study centre who have access to certain medical data concerning children be subject to an obligation of secrecy.

Staff evaluation

Staff evaluation represents a large proportion of the processing operations submitted to the EDPS for prior checking with many processing operations involving probation, appraisal and promotion procedures (see chart on page 23).

A particularly interesting example in the area of evaluation is the EDPS opinion on the European Administrative School (EAS) **Emotional Intelligence 360 degree assessment** at the European Commission (Case 2009-100).

EU institutions and bodies collect and process health data.

A particular concern in the opinions of the EDPS on staff evaluation related to the **retention periods** of personal data following the evaluation exercise.

The EDPS considered that **evaluation reports** should only be kept for five years after the end of the evaluation exercise unless a legal action is pending. Any decisions resulting from these exercises are to be kept in the personal file of the staff member concerned.

The EDPS also concluded in these cases that the **right of rectification** as granted to the data subjects by Article 14 of the regulation could imply the possibility for the data subject to request the insertion of any decision of a Court or other body in the event of a revision of the appraisal or promotion decision.

The purpose of the procedure is to allow participants in EAS training courses to obtain feedback, in the form of a report, to help them enhance their competences in the areas of self-management, relationship management and communication. The exercise is conducted with the use of a web-based tool: 'Emotional IntelligenceView 360'. A report is automatically generated in response to the answers completed by the participants and their colleagues and does not reveal the way in which the colleagues completed the answers.

Even though the EAS has no access to the data processed by the contractor, the contractor has to act according to the instructions given by the EAS. The EDPS therefore considered that the EAS is the data controller of this processing activity because it determines the purposes and the means (the use of the web-based tool). The contractor is therefore not authorised to make any further processing activity beyond what is determined by the EAS and specified in the contract.

The EDPS recommended that the EAS explore the possibilities for making the use of this web tool an anonymous exercise. In this regard, variables such as IT development, procedures and cost would need to be taken into account.

The issue of **working notes** which may be taken during an evaluation meeting by the reporting officer was also addressed by the EDPS (Case 2007-0421). According to the EDPS these notes are taken by the reporting officers in their official capacity, and therefore fall under the applicability of the regulation. Although it is not unlawful to take notes during the evaluation process, it is particularly important that these 'personal notes' do not fall into a grey area without adequate data protection safeguards.

The EDPS considered that any personal notes taken by the reporting officer (and the assessor) during the interviews should be destroyed after drawing up the evaluation report.

Staff evaluation represents a large proportion of processing operations submitted to the EDPS for prior checking

Recruitment

At the end of 2008, the EDPS issued guidelines on the processing of personal data in the framework of recruitment procedures in view of notification of processing operations relating to such processing by EU agencies (see Section 2.7, 'Thematic guidelines').

Specific recruitment procedures at the European Parliament were examined by the EDPS, notably the processing of personal data in the framework of the **hearings of Commissioners designate** (Case 2009-332) and in the **selection of a director for the European Institute for Gender Equality (EIGE)** (Case 2008-785). In both these procedures, data were initially collected by the European Commission and were transmitted to the Parliament, which proceeded to a hearing of candidates. The EDPS paid particular attention to information provided to the candidates by the European Commission when collecting data from candidates.

Recommendations were also made about the conservation of personal data for historical purposes. Although not problematic in the specific selection procedures under examination, the prior-check opinions revealed the lack of a suitable selection and verification process on the basis of criteria determined at an institutional level to only retain data of historical value. The EDPS also made recommendations in the field of security measures.

Performance tools

The **DG ENTR Data Warehouse (EDW)** is a system which retrieves data from multiple data sources in order to process and cross-reference them with a view to obtaining measurements, indicators and reports on the activities of the Enterprise and Industry DG at the European Commission (Case 2008-487). Based on the compiled information, the DG will create reports presenting metrics of performance for the heads of unit, directors and director-general. The system is therefore not designed to measure individual performance of staff members, but to evaluate the performance of the DG as a whole. In this respect, the EDPS underlined that the use of data should be limited to the use specifically declared in the notification, for example to develop a scoreboard for management and to report discrepancies between the different data sources.

The EDPS stressed that this aggregation of databases increases the risk of **function creep** when the interlinking of two (or more) databases designed for distinct purposes will provide a new purpose for which they have not been built, a result which is in clear contradiction of the purpose limitation principle. To be authorised, such a purpose must be clearly limited and the necessity demonstrated. Therefore, the EDW should limit the use to data coming from the databases declared in the notification and require further authorisation if other data sources are to be added.

Time management

Time management systems continued to raise particular interest, specifically when EU institutions and bodies decide to **interface time management systems** with other systems.

The Court of Auditors intended to link the audit management system (ASSYST) with the flexitime system of the Court (EFFICIENT) through the so-called **ART tool** (Case 2008-239). The purpose of the processing operation is to enable individual auditors and their Heads of Unit to reconcile their time recorded in ASSYST with EFFICIENT and to ensure consistency between the two and verify any discrepancies.

The EDPS concluded that since the aggregation of databases increases the risk of 'function creep', such a purpose must be clearly limited and the necessity be demonstrated. In the specific case, the necessity was initially not clearly established and should be further developed. This instrument has since been adopted by the Court of Auditors.

Concerns were also raised by the EDPS in his opinion on an envisaged system **checking flexitime clocking against data on physical access** to the Secretariat-General of the Council (SGC) (Case 2009-477). The SGC uses a flexitime system which records working time and attendance, thereby facilitating the calculation of overtime and leave entitlement. This application had already been prior checked by the EDPS. The SGC also has a system of access control managed by the Security

Time management can raise data protection issues especially when EU institutions decide to interface time management systems with other systems.

Office and accessible to the administration services within the framework of a formal enquiry. The comparison of the two sets of data aims to identify persons who transgress the flexitime rules, and also evaluate their behaviour. The system is also likely to lead to the adoption of disciplinary measures.

In his opinion, the EDPS considered that the necessity and proportionality of checking flexitime clocking data against data on physical access was questionable. According to the EDPS, there is no reasonable evidence showing that the implementation of a system of control comparing clocking times with data on physical access is necessary for the purposes of either personnel management or the functions of the SGC.

The EDPS therefore considered that the envisaged processing would breach the regulation in various ways (necessity and proportionality, change of purpose, quality of the data) unless it was carried out for the purposes of a specific administrative enquiry.

Security investigations

The EDPS analysed procedures put in place to deal with the threats to the Commission interests in the fields of **counter intelligence** and **counter terrorism** (Case 2008-440). Two specific processing operations were scrutinised: **security investigations** and **screening procedures**. Security investigations concern leaks of EU classified information by any employee of the Commission whereas the screening procedures aim at preventing the recruitment or the conclusion of a contract with persons that represent a threat to the Commission interests.

The EDPS welcomed the different measures that were put in place by the responsible unit, notably the fact that the unit primarily assesses, on a case-by-case basis, the **necessity** of the screening procedure following specified criteria. The EDPS recommended that the investigators also bear in mind the **proportionality** criteria when collecting and processing personal data.

Voice logging

*Voice logging of telephone calls raises particular concerns as the recording of calls is a violation of the **principle of confidentiality of communications**.*

The EDPS examined the recording of communications for security purposes at the Joint Research Centre Institute for Energy (JRC-IE) (Case 2008-0014). This case concerned the recording of incoming and outgoing calls (including details of the source and destination number, and the date, time and length of the call) for use in the event of operational incidents, emergencies, the evaluation of emergency training exercises and investigations into potential threats. The EDPS acknowledged that voice logging of telephone calls was lawful based on national legislation relating to nuclear facilities, but recommended that external persons contacting the switchboard be informed that their communication will be recorded for security purposes at the start of the call.

EudraVigilance

The European Medicines Agency (EMA) hosts and manages the EudraVigilance database, which contains **reports on suspected adverse reactions to medicinal products for human use** (individual case safety reports — ICSRs). EudraVigilance facilitates the reporting and evaluation of these reports. National competent authorities, marketing authorisation holders and sponsors of clinical trials provide this information to the EMA.

The EDPS analysed EudraVigilance related data processing operations and emphasised the shared responsibility of the different data controllers involved to ensure the respect of the rights of data subjects (Case 2008-402). Data controllers at both national and EU level must coordinate and join efforts to ensure compliance with national and EU data protection legislation.

The EDPS recommended that the EMA examine the possibility to anonymise or pseudoanonymise personal information contained in ICSRs, and to minimise the personal data in these reports. He also recommended that the EMA, together with the national data controllers, draft a standard notification form to provide the legally required information to individuals, which should include a reference to EudraVigilance.

Waiving of immunity

Under the Protocol on the Privileges and Immunities of the European Communities, officials and other servants of the Communities enjoy a number of immunities. The **Investigation and Disciplinary Office** of the Commission (IDOC) is responsible for evaluating requests from national courts or other national bodies to waive any of those immunities. The EDPS prior checked the procedure put in place by IDOC for the waiving of such immunities (Case 2008-645).

In most cases, IDOC is asked by the national authorities to carry out its investigations in secrecy, which limit the rights of the data subjects as they are not informed about the investigation, nor can they exercise their rights of access and rectification during the course of such investigations. The EDPS outlined that any limitation of data subjects' rights must be temporary and that the data subject must be able to exercise their right of access as soon as secrecy is no longer justified.

Following the investigation, IDOC transfers its decision and certain data to the requesting court/national authority. The EDPS recommended that IDOC maintain a list of the recipients of these data, recording the legal justification for the transfers.

Since the waiving of immunity is usually part of a wider procedure which may or may not lead to other actions, the EDPS recommended that the file retention periods be reduced where disciplinary and/or court procedures are dropped or the data subject is acquitted.

Pilot projects

In three cases involving pilot projects, the EDPS took the opportunity to remind institutions and agencies of **the rules governing the prior checking of pilot projects**. By providing recommendations prior to the full deployment of a system, the EDPS wants to minimise subsequent modifications by the data controller.

> The results of the pilot project must be analysed and communicated to the EDPS prior to the launch of the general project and the EDPS must be informed of any modifications that are likely to have an impact on the processing of personal data. The prior-checking opinion should be seen as closing the full analysis of the pilot project.

2.3.4. Consultations on the need for prior checking

During 2009, the EDPS received 21 consultations from DPOs on the need for prior checking (on the basis of Article 27(3) of the regulation), including 11 from the DPO of the European Parliament.

*Several cases were declared **subject to prior checking**, for example:*

- *strike-related data at the European Central Bank;*
- *hearings of Commissioners-designate at the European Parliament;*
- *ergonomical assessment of work environments at the European Parliament;*
- *senior staff appointments at the European Parliament.*

The processing of personal data by the **legal service and the legal affairs unit of the European Parliament** in the context of their respective duties of examining cases, preparing replies to requests and complaints, and legal proceedings was not considered to be subject to prior checking by the EDPS (Case 2009-263).

The mere possibility of the presence of **sensitive data** does not automatically make it a case for prior checking. Nevertheless, the presence of sensitive data in the handling of those cases such as health-related data or data relating to offences does mean that particular attention should be given to the

adoption of security measures in accordance with Article 22 of the regulation.

Although some of the processing operations could be related to an evaluation of personal aspects, the processing is not intended to evaluate the data subject and so Article 27(2)(b) does not apply.

Likewise, in relation to Article 27(2)(d), although the processing operations could result in excluding an individual from a right, benefit or contract, this is not their specific and sole purpose.

The EDPS was also consulted on the processing of personal data in the course of the **selection procedure of assistants of MEPs**. According to information received, the selection procedure is not carried out by the Parliament, and the EDPS therefore considered that the processing operation should not be submitted for prior checking. The EDPS nevertheless highlighted that this does not mean that the MEP assistants do not enjoy certain data protection rights which must be guaranteed by the European Parliament.

2.3.5. Notifications not subject to prior checking or withdrawn

In 2009, the EDPS also dealt with 21 cases which, after careful analysis, were found not to be subject to prior checking. In these situations, the EDPS may still make recommendations.

Youthlink 2

An interesting case concerned **Youthlink 2**, the main repository of (statistical and financial) data concerning projects and activities submitted under the 'Youth in action' (YiA) programme at the European Commission (Case 2008-484).

The EDPS concluded from the facts received, that the selection of beneficiaries for the 'Youth in action' programmes **did not involve an evaluation of individual conduct or abilities**, but was rather a check on the proposed project against predefined criteria and a check of the financial and operational capacity of the applicant legal entities or groups. In addition, such an assessment is carried out in a decentralised way — not by the data controller within the European Commission but either by national agencies subject to their respective data protection legislation or by the EACEA. For these reasons, the EDPS did not find Article 27(2)(b) of the regulation applicable.

Customer satisfaction surveys

The EDPS considered that **customer satisfaction surveys** at the European Central Bank were **not subject to prior checking** as the purpose of the surveys is not to evaluate individuals, but rather services, much the same way as the purpose of an audit is to evaluate compliance of the work of an organisational unit or a process, rather than to evaluate the performance of individuals (Case 2008-780). The ECB had made efforts to minimise the chances that any evaluation of personal aspects of an individual may occur. Nevertheless the EDPS suggested that the ECB take further steps to minimise the possibility that some personal information may be included in the survey results, in particular those that may originate in the responses given to open questions.

Use of mobile phones

In relation to the notification on the **use of mobile phones** by the Executive Agency for Competitiveness and Innovation (EACI) staff going on mission, the EDPS concluded that the case **was not subject to prior checking** (Case 2009-162). The purpose of the processing was to ensure that costs for private calls are reimbursed to the EACI. Assessing of staff members' ability, efficiency or conduct was therefore outside the remit of the processing and it did not fall under Article 27(2) (b).

Identity and access management

The EDPS also considered that the Court of Auditors' **identity and access management system** was not subject to prior checking (Case 2009-639). Although the system uses certain information (name, surname, birth date) in order to grant users application accounts and access to such accounts, it does not 'evaluate' individuals, but rather authenticates their identity and access rights. The mere checking of the rights based on pre-defined rules does not therefore entail a *de facto* evaluation of a user's efficiency, competences, ability to work or behaviour, and hence does not qualify the case under Article 27(2)(b).

2.3.6. Follow-up of prior-checking opinions

*An EDPS prior-check opinion will include **recommendations** which must be taken into account in order to make the processing operation comply with the regulation. 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 in Regulation (EC) No 45/2001. In particular, the EDPS may refer the matter to the Community institution or body concerned.*

Most prior-checking cases have led to recommendations mainly concerning:

- information to data subjects;
- data conservation periods;
- purpose limitation;
- the rights of access and rectification.

Institutions and bodies are willing to follow these recommendations and, up to now, there has been no need for executive decisions. The EDPS requests in the formal letter sent with his opinion that the institution or body concerned informs the EDPS of the measures taken to implement the recommendations within a period of three months.

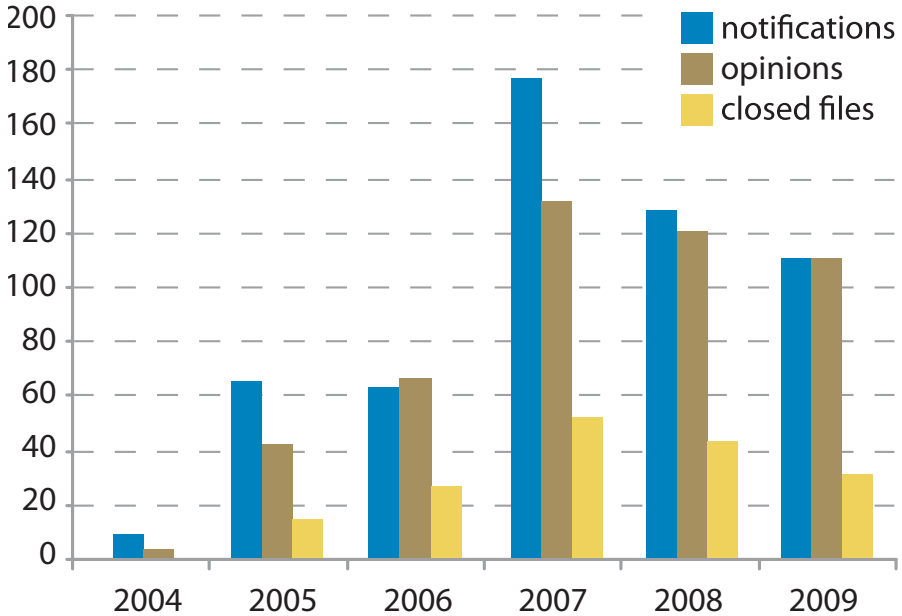
Despite reminders to institutions and bodies to provide such feedback, during 2009 the EDPS closed only 32 cases, leaving a number of cases still open. The EDPS has therefore urged institutions and bodies to proceed with the follow-up of his opinions so that he may close the case accordingly.

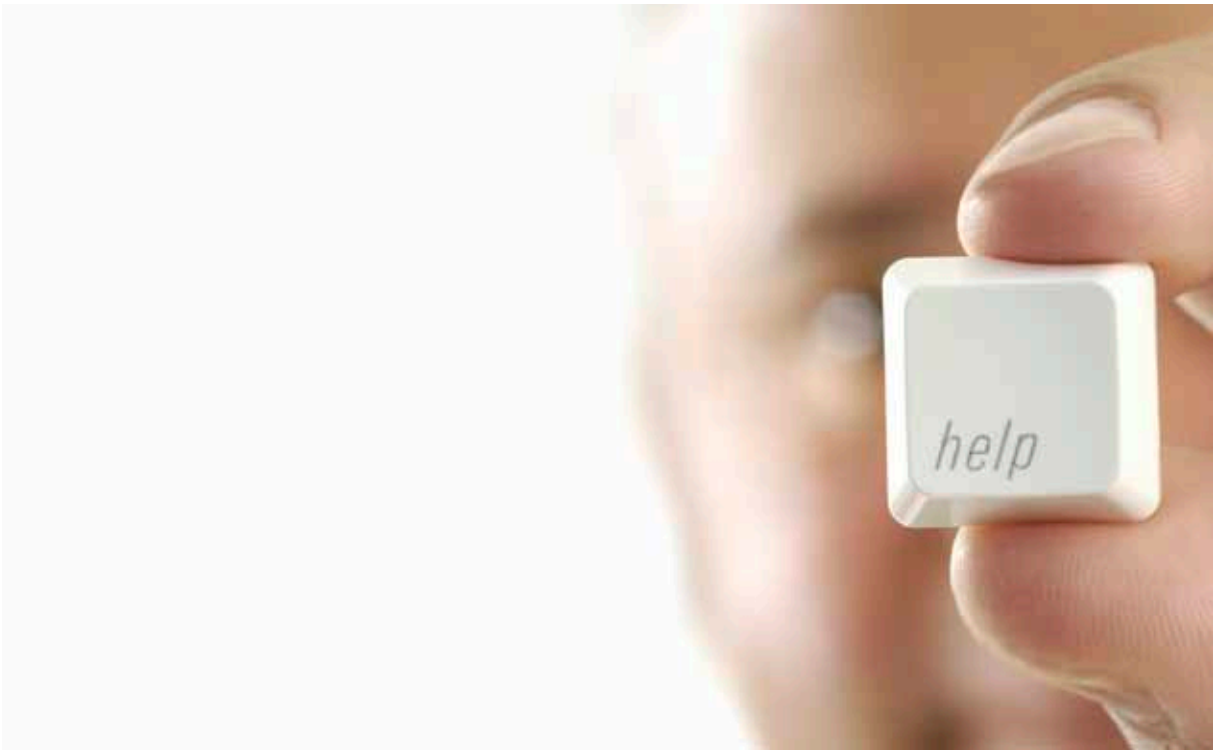
2.3.7. Conclusions and the future

Most of the main institutions are reaching the end of notifying their existing processing operations and most agencies are making progress in notifying core business operations involving the processing of personal data and standard administrative procedures (in accordance with the new procedure set for the agencies).

The 110 adopted opinions have given the EDPS a good insight into the European administrations' processing operations and enabled him to highlight his recommendations. The experience gathered in the application of the regulation has also enabled the EDPS to gain expertise and provide generic guidance in certain areas (see Section 2.7, 'Thematic guidelines').

Comparative situation





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

Most prior-checking cases have led to recommendations from the EDPS and require feedback from the institutions and bodies on how these recommendations have been implemented. In 2009, few cases were closed and the EDPS will therefore continue pushing for further improvements in this field.

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).

In an interesting case related to **data of a minor**, the EDPS considered that a child's data can, in principle, be accessed by a parent who exercises legitimate parental authority. The case concerned access to documents relating to registration of a child at a crèche managed by an EU institution. The complainant alleged that he was not provided full access to these documents submitted by the other parent from whom he was divorced. In particular, the names of the persons authorised to collect the child from the crèche were partially redacted.

The EDPS stated that, in principle, the parent who exercises legitimate joint parental authority has the right to obtain access to the data of his or her child. In this case, the EDPS concluded that such rights also covered data of third parties authorised to collect the child, since such data were by their nature connected to that of the child.

The EDPS considered that by refusing to give the complainant access to his child's data in an intelligible manner, the institution in question was in breach of Article 13 of the regulation.

According to the regulation, the EDPS can only investigate complaints submitted by **natural per-**

sons. Complaints submitted by businesses or other legal persons are not admissible. Complainants must also identify themselves and so anonymous requests are not considered as a 'complaint'. However, anonymous information may be taken into account in the framework of another procedure (such as a self-initiated enquiry, or a request to notify 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.*

In particular, the fact that the regulation mentions 'rectification of personal data' does not mean that the EDPS is competent to revise the substance of decisions because they contain some personal data. In such cases the complainant is advised to either turn to the European Ombudsman or to the competent Court.

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

2.4.2. Procedure for handling of complaints

The EDPS handles complaints according to the existing legal basis, the general principles of EU law and the good administrative practices common to EU institutions and bodies. In order to facilitate complaints handling, in December 2009, the EDPS adopted an **internal manual** designed to provide guidance to staff when handling complaints. In particular, the EDPS conducted a thorough review of the conditions for admissibility of complaints. During 2009, the EDPS also implemented a **statistical tool** designed to monitor complaints related activities, and in particular to monitor the progress of particular cases.

In all phases of handling a complaint, the EDPS adheres to the principles of proportionality and reasonability. Guided also 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 have or may have suffered as a result of the violation;
- the potential overall importance of the case, also in relation to the other public and/or private interests involved;
- the likelihood of establishing that the infringement has occurred;
- the exact date when events happened, 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** will be declared inadmissible and the complainant informed accordingly. In such cases, the EDPS informs the complainant about any other competent bodies (e.g. Court, Ombudsman, national data protection authority, etc.).

A complaint that addresses facts which are **manifestly insignificant**, or would require **disproportionate efforts** to investigate is not investigated further. 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 an analysis of which other options are available to deal with the relevant issue, either by the complainant or by the EDPS. For instance, the EDPS can open an own-initiative inquiry on a general problem instead of opening an investigation on an individual case submitted by the complainant. In these cases the complainant is informed about such other means of action.

*The EDPS was informed anonymously about the fact that personal data of candidates who pass the **pre-selection tests** in competitions for EU civil servants are processed by an **external contractor located in a non-EU country**. The EDPS opened an inquiry into this case on his own initiative, which led to the conclusion that in fact, even though the European Personnel Selection Office (EPSO) had concluded a contract with an external firm registered in the United Kingdom, the data processing operations themselves were performed in the United States. The EDPS requested EPSO to verify if all the conditions laid down in Article 9 of the regulation are respected and to amend the contract in order to reflect additional guaranties for the data subjects concerned.*

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 — i.e. 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 brought forward should not be reopened by the other institution unless significant new evidence is submitted.

As to the **time limits**, if the facts addressed to the EDPS are submitted with a delay of more than two years, the complaint is in principle inadmissible. The two-year period starts from the date at which the complainant had knowledge of the facts.

Where a complaint is admissible, the EDPS will carry out **an inquiry** to the extent which he believes appropriate. This inquiry can include an information request 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 be granted access to any premises in which a controller or institution or body carries on 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 position about 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 in the General Court (Cases T-164/09 and T-193/09).

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 work in a **transparent manner** and to publish at least the substance of his decisions. The internal procedures of the EDPS reflect this difficult balance.*

As a 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 into all correspondence between the EDPS and the institution.

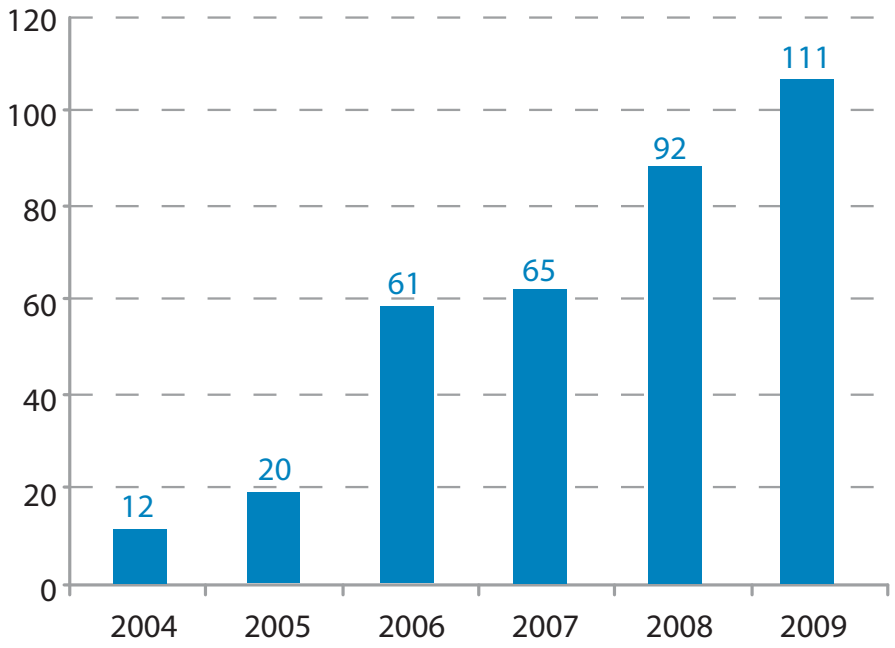
If the complainant requests **anonymity** from the institution, the DPO or third parties involved, he or she is invited to explain the reasons for such a request. The EDPS then analyses the complainant's arguments and examines the consequences for the viability of the subsequent EDPS inquiry. If the EDPS decides not to accept the anonymity of the complainant, he explains his evaluation and asks the complainant whether he accepts that the EDPS examine 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 to notify a data processing operation.

After the end of an inquiry, all **documents related to the complaint**, including the final decision, remain in principle confidential. They are not published in full or transferred to third parties. However, an anonymous summary of the complaint can be published by the EDPS on its 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 form which takes into account any complainant's request for confidentiality and would therefore not allow the complainant or other concerned persons to be identified.

2.4.4. Complaints dealt with during 2009

2.4.4.1. Number of complaints

Number of complaints received (evolution 2004–2009)



Both the number and complexity of complaints received by the EDPS is increasing. ***In 2009, the EDPS received 111 complaints*** *(an increase of 32 % compared with 2008). 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 42 complaints required more in-depth inquiries (an increase of 83 % compared with 2008). In addition, 14 admissible complaints submitted in previous years (13 in 2008 and 1 in 2007) were still in the inquiry or review phase.*

2.4.4.2. Nature of complainants

Of the 111 complaints received, 26 complaints (23 %) were submitted by members of staff of EU institutions or bodies, including former staff members and candidates for employment. One complaint was anonymous and for the remaining 84 complaints, the complainant did not appear to have an employment relationship with the EU administration.

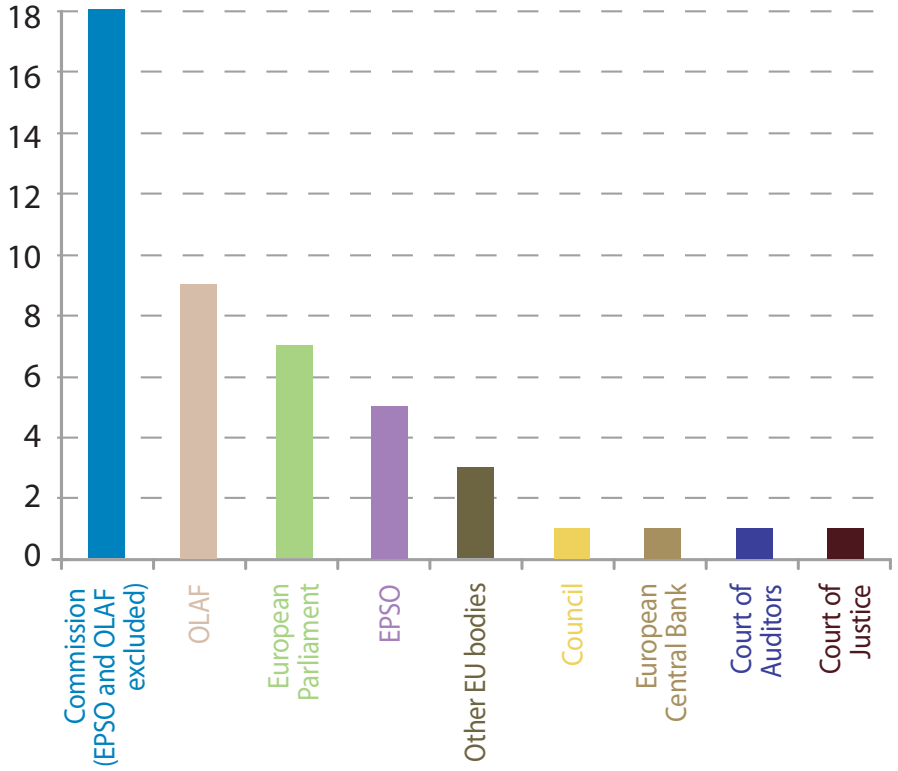
2.4.4.3. Institutions concerned by complaints

Of the admissible complaints submitted in 2009, the majority (over 70 %) 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 high number of complaints related to OLAF and EPSO may be explained by the nature of the activities undertaken by those bodies.

2.4.4.4. Language of complaints

The majority of complaints were submitted in English (64 %); German (19 %) and French (9 %) being less commonly used. Complaints in other languages are relatively rare (8 %).

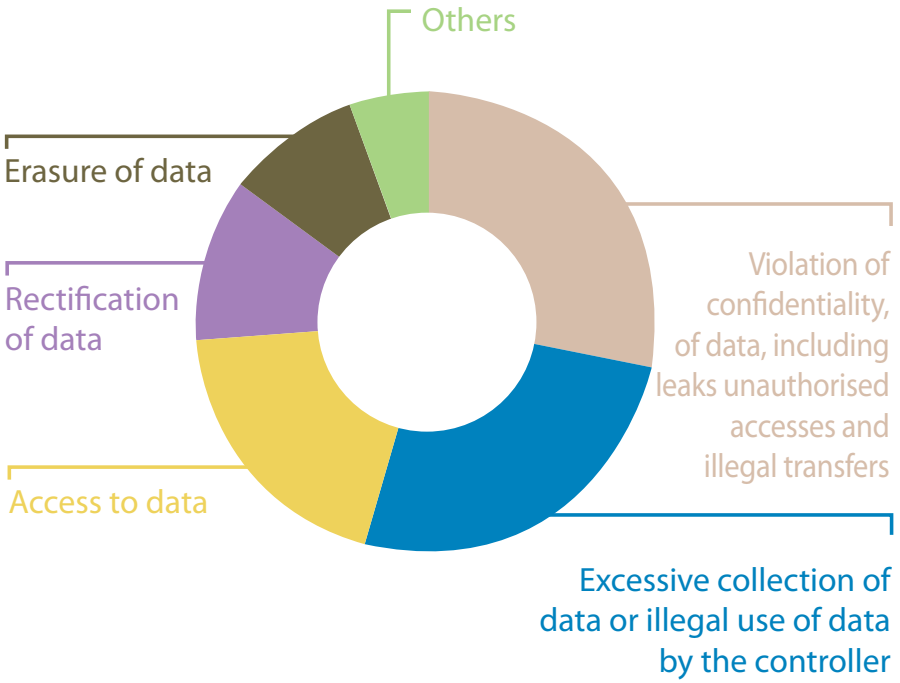
Institutions concerned



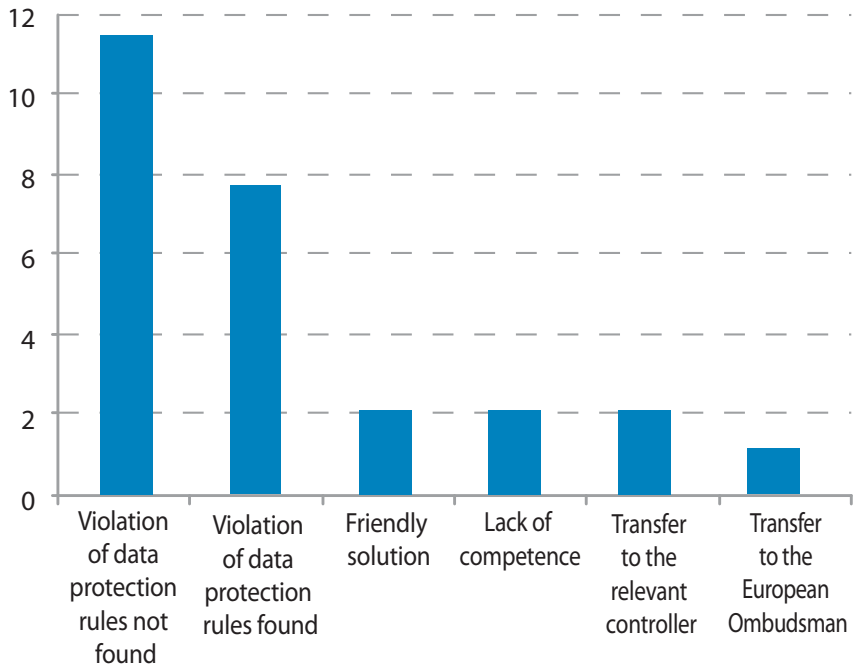
2.4.4.5. Types of violations alleged

The main types of violations of data protection rules alleged by the complainants in 2009 were: violation of confidentiality of data, including leaks, unauthorised accesses and illegal transfers (31 %) and excessive collection of data or illegal use of data by the controller (28 %). Other violations were alleged less frequently, specifically access to data (20 %), rectification of data (12 %), erasure of data (10 %), video-surveillance (2 %), transfer of data outside the EU (2 %) and loss of data (2 %).

Types of violations alleged



Result of EDPS enquiries



2.4.4.6. Results of EDPS enquiries

In 12 cases resolved during 2009, the EDPS found no breach of data protection rules.

In a case against the European Commission, a former staff member complained about a refusal to provide him with a copy of a report concerning an administrative inquiry conducted by the Commission. The Commission refused to provide access to the full text of the report, justifying its refusal by the necessity to protect the rights and freedoms of others, in particular witnesses who had testified in this case. However, it did provide the complainant with access to the factual findings concerning him and to the final conclusions of the report. Given the fact that release of the full text could indeed adversely affect some of the individuals concerned, the EDPS considered that the actions of the Commission fulfilled the requirements of Article 13 of the regulation, whilst preserving the rights and freedoms of others.

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

In one case, a staff member complained about impropriety by a body in relation to an investigation into the staff member's professional qualifications. The complainant alleged that his employer illegally transferred 'confidentially-marked' documents evidencing the qualifications to a number of recipients both within and outside EU institutions.

On the basis of the information provided by the data controller, the EDPS concluded that the intra-EU transfers were necessary in order for the recipients to legitimately perform their tasks. With regard to transfers to third parties, while the EDPS was satisfied that such transfers were done in accordance with Article 8, he did find that the transfer to a media consultancy (hired to deal with possible press coverage of the investigation) was excessive in view of the tasks performed by that recipient. The EDPS thus concluded that such a data transfer was in breach of the data quality principle and that the relevant EU body in so far violated Article 4(1)(c).

In two cases, the EDPS contributed to an informal solution between the complainant and the institution concerned and no decision was signed.

2.4.5. Further work in the field of complaints

The adoption of the **internal manual for complaint handling** in December 2009 facilitated the revision of the relevant pages of the EDPS website. The new page describes the main elements of the procedure and includes a downloadable form for the submission of complaints, together with information on admissibility. This information was made available on the EDPS website in early 2010 and will help potential complainants submit a complaint. It is also expected to limit the number of obviously inadmissible complaints and provide the EDPS with more complete and relevant information enabling more effective complaint handling. It is hoped that an interactive version of the complaints form will follow, allowing users to complete it on screen and then send it automatically to the EDPS.

2.5. Monitoring compliance

The EDPS is responsible for monitoring and ensuring the application of Regulation (EC) No 45/2001 (Article 41(2) of the regulation). Monitoring was notably performed by a reporting exercise referred to as 'spring 2009'. This exercise was a continuation of a similar initiative (spring 2007) and took the form of letters addressed to directors of EU institutions and bodies to request updates on progress made in certain fields. In addition to this general monitoring exercise, inspections were carried out on certain institutions and bodies to verify compliance on specific issues.

2.5.1. 'Spring 2009' exercise

Following the exercise, the EDPS issued a second general report measuring progress made in the implementation of data protection rules and principles by EU institutions and bodies. The report shows that generally EU institutions have made good progress in meeting their data protection requirements although a lower level of compliance is observed in agencies.

Main results in institutions

- **Inventory of processing operations:** the EDPS is satisfied that all but one institution have drafted an inventory of processing operations involving personal data, which allows a more systematic approach to implementation.
- **Notification of processing operations from data controllers to the DPO:** the EDPS notes an increase in the number of institutions which have completed the process. By the end of 2008, at least six institutions could claim that all processing operations had been notified to the DPO, compared with only two institutions in the beginning of 2008.
- **Notification of processing operations to the EDPS for prior checking:** only two institutions have so far managed to notify all existing processing operations to the EDPS for prior checking. However, most institutions indicated that all identified processing operations would be notified to the EDPS by the end of 2009.

Main results in agencies

The EDPS observed that **positive progress** had been made in the identification of processing operations and in the adoption of implementing rules concerning the tasks and duties of the DPO. However, the level of notifications of processing operations to the DPO and further notifications to the EDPS for prior checking was generally very low. Only one agency claimed that all identified operations had been notified to the EDPS.

Although there have been no or very few requests for access to data under the regulation, the EDPS was pleased to note that the agencies are considering setting up monitoring tools to keep track of these requests.

Further 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 to the EDPS and notifications to the DPO needs to be improved. Additional enquiries regarding compliance will follow in order to assess further progress.

2.5.2. Inspections

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

The extensive powers to access any information and personal data necessary for his inquiries and to obtain access to any premises where the controller or EU institution or body carries out its activity are designed to ensure that the EDPS has sufficient tools to perform his function. Inspections can be triggered by a complaint or be carried out at the EDPS's 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 2009, the EDPS continued the inspections announced in the framework of the spring 2007 exercise, notably at the European Parliament and EPSO, and also launched an inspection at the European Court of Auditors. In July 2009, on the basis of experience gathered during inspections, the EDPS adopted an internal inspection procedure manual and published the key elements of this procedure on the EDPS website.

EDPS inspection policy and procedure

The EDPS **internal staff manual on inspections** aims to provide guidance for EDPS staff. It is essentially based on the existing legal framework, general principles of EU law, and the good administrative practices common to the EU institutions and bodies.

The manual contains details of the administrative procedure, the tasks of inspectors, and the security policy as well as standard forms for producing inspection documents. It explains the purposes of these documents and gives useful tips for the preparation of an inspection.

The inspection manual is a living document, subject to regular revision as EDPS practices and experiences evolve. A policy document on the role of inspections and on the criteria for undertaking an inspection will be developed in due course.

Inspection at the European Parliament

In February 2009, the EDPS conducted an inspection at the European Parliament. The inspection aimed to investigate the facts relating to the personal data processing operations of both the medical services in Brussels and Luxembourg, and the Medical Absences Service, in relation to three prior-checking opinions issued by the EDPS. It also aimed to check the implementation of the recommendations made in those opinions. The obligation of the data controllers at the Directorate-General for External Policies to notify the DPO about personal data processing operations under Article 25 of the regulation also formed part of the inspection.

Following the inspection, the EDPS expressed concerns regarding a number of deficiencies in the field of **information security in the medical services** (i.e. organisational, physical and technical), suggesting that substantial improvements are necessary. In particular, the EDPS requested that a proper solution be found for the transfer of medical reports from the Medical Absences Service to the medical service.

The EDPS sent a list of recommendations to the Secretary-General of the Parliament and requested that he take appropriate measures. A number of these measures have subsequently been implemented but the follow-up of this inspection still continues.

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 aimed to investigate the facts regarding the personal data processing operations in relation to several prior checks in the field of the selection of officials, temporary staff and contract agents and any related personal data processing operations.

The inspection showed that EPSO had made considerable **progress in relation to the transparency** of their procedures and information provided to candidates. In its conclusions, the EDPS did, however, reiterate the obligation for EPSO to provide the evaluation sheets produced by the jury in the

oral exams to those candidates who requested them. The issue of access to the questions in the multiple choice tests was not examined during the inspection as this is currently before the Court.

As regards the **conservation policy**, the EDPS called for a documented procedure for the archiving of files in the historical archives of the Commission.

The inspection also aimed to check the compliance of some **selected EPSO databases and IT tools** used in the selection procedures. As a general measure, the EDPS requested that the technical and organisational security measures be documented and more systematically integrated into the competition procedures.

The conclusions of the inspection were sent to the Director of EPSO who has adopted an action plan for recommendations made by the EDPS. Given that this action plan is part of a continuous improvement plan and that procedures are accordingly being reviewed, the EDPS has reserved his final conclusions until the beginning of 2010.

Inspection at the European Court of Auditors

In March 2009, the EDPS carried out an inspection at the European Court of Auditors (ECA) in relation to **monitoring staff** (Internet monitoring and audit tool report).

The EDPS welcomed the ECA's use of **filtering techniques** that facilitate a preventive approach to the misuse of the Internet rather than a repressive one. Notably, the EDPS rejected the features and functions of software filters used to monitor failed attempts to access the Internet and highlighted the importance of **privacy impact assessments** as a tool to be used in the selection process of software for monitoring purposes. The EDPS also considered it best practice to extend the principles of **privacy by design** to the entire design process of Internet and network monitoring systems and processes. The EDPS urged the ECA to improve policies designed to maintain a **high security policy compliance level** in order to build an Internet monitoring procedure which is solid, secure, fair and respectful of privacy and data protection rules.

Regarding the aspect of the inspection relating to the consultation on a procedure to access private drive/e-mail of staff members, the EDPS analysed the relevant purposes and current practices at the ECA and concluded that there was a risk of breaching the confidentiality of communications. As a consequence, the EDPS stressed that a formal notification for prior checking be submitted to him on this processing operation as it gave rise to a specific risk under Article 27(1) of the regulation.

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.

The EDPS, as the supervisory authority of the European Commission's IT systems and applications which process personal data, decided to carry out an inspection of the s-TESTA network and more specifically of its Service and Operational Centre (SOC) in Bratislava in September 2009. The European Commission entrusted the management of the SOC to a contractor, Orange Business Service/ Hewlett Packard (OBS/HP). The main objective of the inspection was to gather facts on the security and data protection measures implemented, and compare them with the requirements defined in the contract and corresponding regulations. Within this framework, the EDPS inspection applied to the SOC infrastructure, personnel, organisation and technologies.

The EDPS was generally satisfied with the security measures requested by the Commission and implemented by OBS/HP on the IT systems, applications and organisational processes of the SOC. The launching of various security upgrades and the implementation of a continuous improvement plan will offer an even stronger data protection mechanism.

2.6. Administrative measures

*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 his 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 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 were raised, including for example:

- transfers of personal data to third countries;
- processing of personal data in the framework of a pandemic procedure;
- the exercise of the right of access;
- application of the data protection rules to the Internal Audit Service;
- implementing rules of Regulation (EC) No 45/2001.

2.6.1. Transfers of personal data to third countries

The **European Anti-Fraud Office** (OLAF) raised the question of whether three groups of countries can be considered to have an **adequate level of data protection**, in the light of their relation to Council of Europe Convention 108 and its Additional Protocol.

OLAF also asked — should one or more of these groups not be considered to have an adequate level of protection within the meaning of the data protection regulation (Article 9.1) — whether the commitments they have undertaken in the context of the convention and/or mutual administrative assistance agreements in customs matters would be considered as 'adequate safeguards' (Article 9.7) (Case 2009-0333).

Following analysis, the EDPS concluded that there was **not sufficient evidence** of the satisfactory implementation of Convention 108 and its Additional Protocol, in the countries concerned. Therefore, in principle, the three groups of countries could not be considered to have an adequate level of protection.

The EDPS added that OLAF could nevertheless consider carrying out an assessment of whether a particular transfer (or a set of transfers) can be made, limited to specific purposes and recipients in the country of destination that would effectively provide an adequate level of protection. Such an assessment would involve a review of the national law that implements the convention and its protocol and their effective implementation.

The EDPS also mentioned that a third course of action could be for OLAF and recipients to introduce adequate safeguards.

2.6.2. Processing of personal data in the framework of a pandemic procedure

The EDPS was consulted on the issue of processing of personal data by the **European Central Bank** (ECB) in the event of a **pandemic** (Case 2009-0456). Apart from the processing of personal data by the medical services of the ECB, the pandemic would also require informing local management that a specific person was suspected of being infected so that the relevant team members could be warned.

The EDPS considered that, in the absence of any national legal obligation, Article 5(a) of the regulation could serve as legal basis for the processing of data in the framework of the pandemic procedure. However, as this is exceptional, it would be desirable that the ECB take a formal decision on which any communication to management could be based.

The EDPS further underlined that, as the processing concerned health-related data, the processing was prohibited unless exceptions could be found in compliance with Article 10. The processing of health-related data could be based on a legal obligation for employers to comply with obligations on health and safety at work. The EDPS also considered that in the present case reasons of 'substantial public interests' could justify this processing of health data, but that adequate safeguards must be put into place to protect the interests of the data subjects.

2.6.3. The exercise of the right of access

The EDPS was consulted by **OLAF** on a hypothetical case related mainly to the exercise of the **right of access** (Case 2009-0550).

The EDPS considered that the request for a list of cases in which personal data of the data subject appear would, in principle, be covered by Article 13(a) of the regulation, since it is a way to obtain 'confirmation as to whether or not data related to him or her are being processed'. The way in which the 'confirmation' could be provided depends, to a certain extent, on the nature and characteristics of the data and the processing activity involved. It also depends on whether or not a particular way of providing the confirmation would allow the data subject to exercise his or her different data protection rights ([7]).

A case-by-case approach should be followed in the assessment of the access methods and parameters. The information provided to the data subject must be 'understandable' (in an 'intelligible form'), stating which processing activity is taking place and which data are involved. The level of detail should allow the data subject to evaluate the accuracy of the data and the lawfulness of the processing, as well as reflect the burden of the task for the controller.

2.6.4. Application of data protection rules to the Internal Audit Service (IAS)

In view of an upcoming audit on human resources management at the European Medicines Agency (EMA), the Head of Administration of EMA requested that the EDPS confirm whether the regulation is applicable to the IAS team during the course of the audit (Case 2009-0097).

The EDPS considered that IAS is a Community body processing personal data in the framework of the exercise of activities which fell under the scope of Community law, as applicable at that stage, and therefore should the IAS have access to personal data during its auditing activities, the rules provided for in the regulation would be applicable.

2.6.5. Implementing rules of Regulation (EC) No 45/2001

Various DPOs submitted consultations to the EDPS on drafts regarding the implementing rules of Regulation (EC) No 45/2001 by their agencies. The EDPS noted that all drafts addressed not only the tasks, duties and powers of the DPOs (Article 24(8) and annex of the regulation), but also covered the role of controllers and the rights of data subjects. Some recommendations of particular importance made by the EDPS concerned the following issues.

- The DPO should ensure the internal application of the provisions of the regulation in **an independent manner**, without receiving any instructions from anyone (Cases 2009-0656 and 2009-0684).
- The DPO may obtain **external assistance** as long as this does not jeopardise his/her independence (Case 2009-0656).
- If necessary, **training on data protection** should be organised by the agency (Case 2009-0656);
- The staff providing support to the DPO should be bound by the same duty of **professional secrecy** as the DPO (Case 2009-0684).
- The **Staff Committee** should also be able to consult the DPO, and in general the latter can be consulted without going through the official channels (Cases 2009-0684, 2009-0204 and 2009-0163).

([7]) See point 57, judgment of the ECJ in C-553/07, *Rotterdam* v *Rijkeboer*.

2.7. Thematic guidelines

The experience gathered in the application of Regulation (EC) No 45/2001 has enabled EDPS staff to translate their expertise into generic guidance for institutions and bodies. During 2009, the EDPS developed guidance on specific topics in the form of thematic papers.

2.7.1. Guidelines on recruitment

The EDPS guidelines on the processing of personal data in relation to recruitment (adopted at the end of 2008) examine the cycle of administrative procedures (selection, recruitment and contractual arrangements) put in place to recruit permanent, contract and temporary staff, as well as national experts and trainees.

Among others things, the guidelines analyse **the collection** by the institutions of data related to **past convictions** in order to comply with the Staff Regulations: a member of staff may be recruited only on condition that they enjoy the full rights of citizens and can produce the appropriate character references as to their suitability for the performance of their duties. The EDPS considered the collection of data related to criminal convictions as lawful. He nevertheless highlighted that the manner of collecting them — through different documents such as criminal record, police record or certificate of good conduct — may lead to the collection of excessive data. Indeed, these documents may contain information that goes beyond the legitimate purpose of verifying that the person enjoys his or her full rights.

The guidelines therefore recommend that the analysis of the content of such documents is carried out on a case-by-case basis so that only relevant data are processed in the light of the Staff Regulation's requirements.

As to the **retention period** of data related to criminal convictions, the guidelines insist on returning the criminal record to the person immediately after the selection and possible recruitment. These documents are a snapshot which may no longer be accurate the day after their production. For evidential and auditing purposes, a standard form could be created, stating that the person is suitable for the performance of his or her duties and enjoys full rights as a citizen.

The guidelines also analyse the **external transfers** of data either to companies organising tests on behalf of the selection committee or to external experts recruited as members of the selection committee. The necessity of such transfers should be established in compliance with Article 8(a). Furthermore, the precise mandate of external contractors should be established in a contract or a legal act, and their confidentiality and security obligations should be assured in accordance with Article 23 of the regulation.

When recruiting staff, EU institutions should ensure that they only collect relevant data.

2.7.2. Guidelines on health data

In September 2009, the EDPS issued guidelines on the processing of health data in the workplace by EU institutions and bodies.

The guidelines examine the **legal basis** of the processing of health data by EU institutions and bodies as principally established in the Staff Regulations, and determine for what purposes and under which conditions health data can be processed. For example, the Staff Regulations provide for the processing of health data in relation to a pre-recruitment medical examination in order to determine whether or not the future staff member is physically fit to perform his/her duties. The Staff Regulations do not, however, foresee that the same pre-recruitment medical examination could also serve for prevention purposes. Having said this, the EDPS recognises that the data collected during this medical examination could additionally serve to alert a future member of staff to a specific issue concerning his/her health and therefore could serve for prevention purposes. This does not, however, imply that additional data should be requested for the purpose of prevention.

The guidelines also apply **the principle of data quality**. This principle implies an evaluation of all medical questionnaires submitted to staff members to ensure that only the necessary and relevant data are collected and processed. If the data subject is offered the possibility to perform an HIV test during their medical visit, it must be clearly specified that this test is not mandatory and that it may only be based on the specific and informed consent of the data subject. The principle of data quality also leads the EDPS to conclude that, should a staff member decide to have his or her annual medical check-up performed by a practitioner of his/her choice, the results of this visit should only be communicated to the institutions' medical service with the freely given and informed consent of the data subject.

2.7.3. Guidelines on video-surveillance

On 7 July 2009, the EDPS published a consultation version of video-surveillance guidelines. All stakeholders were invited to provide written feedback and a workshop was organised in Brussels on 30 September 2009. Nearly a hundred data protection officers, security officers, video-surveillance and information technology specialists as well as staff representatives from over 40 EU institutions and bodies participated.

The workshop and the consultation process achieved its twin goals of eliciting feedback to

Giovanni Buttarelli, Assistant Supervisor, speaking at the EDPS workshop on draft video-surveillance guidelines (Brussels, 30 September 2009).

improve the draft guidelines and increasing cooperation to ensure compliance with data protection principles. The overall response to the draft guidelines was positive. In a climate of increasing concern over the rise in the use of surveillance, participants welcomed the fact that the draft guidelines provide practical advice for deciding whether to use video-surveillance equipment and how best to address data protection issues.

Objectives of the video-surveillance guidelines and key principles

The EDPS aimed to issue these guidelines at the beginning of 2010 with the dual purpose of: (i) contributing to reducing and preventing uncontrolled proliferation of video-surveillance in cases where it is unwarranted, and (ii) assisting institutions in using video-surveillance responsibly and putting safeguards in place when the use of video-surveillance is justified.

Key topics addressed in the guidelines
- *How to select, site and configure a system*
- *How long should recordings be kept?*
- *Who should have access to the images?*
- *What security measures should be taken to protect the data?*
- *How to inform the public*
- *How to fulfil access requests*

The guidelines are designed to encourage local decision-making based on local security needs, while taking into account the specific concerns of other stakeholders, including staff. They also emphasise the institutions' accountability and recommend adopting a formal video-surveillance policy and carrying out periodic audits to ensure and demonstrate compliance. Finally, they encourage institutions to build privacy and data protection into their deployed technology as well as into their organisational practices, following the principle of 'privacy by design'.

Necessity and proportionality

The guidelines are built on the principles of necessity and proportionality, which, in turn, should lead to data minimisation and help stop the uncontrolled proliferation of security cameras. Decisions on whether to install cameras and how to use them should not be made solely on security needs. Rather, security needs must be balanced against respecting the fundamental rights of the individual.

Questions to ask before installing a system
- *What are the benefits of using video-surveillance?*
- *Is the purpose of the system clearly specified, explicit and legitimate?*
- *Is there a lawful ground for the video-surveillance?*
- *Is the need for video-surveillance clearly demonstrated?*
- *Is it the best way to achieve its intended purpose?*
- *Are there less intrusive alternatives?*
- *Do the benefits outweigh the detrimental effects?*

That said, data protection should not hamper law enforcement authorities from doing their job. Security needs and data protection are often portrayed as opposing concerns that are hard to reconcile. However, fundamental rights and security do not have to be mutually exclusive. Using a pragmatic approach based on the twin principles of selectivity and proportionality, surveillance systems can meet security needs while also respecting privacy. Surveillance technology should be used in a targeted way thus minimising the collection of irrelevant data. This not only minimises intrusions into privacy, it also helps ensure a more targeted, and ultimately, more efficient, use of surveillance to address a security problem. In conclusion, the EDPS sees the need for a selective approach to using surveillance systems so that the public does not suffer excessive limitations as a result of the actions of a minority.

'Privacy by design' and accountability

Privacy and data protection cannot be assured solely by 'ticking' compliance boxes. Whenever possible, a preventive approach must be used: privacy must be 'designed' into information and communication technology (ICT) systems and organisational practices from the outset. 'Privacy by design' extends not only to the design and technical solutions of ICT systems, but also requires accountable, privacy-friendly organisational practices and privacy-friendly physical infrastructure. Video-surveillance is an area where the principles of privacy by design can be particularly useful and relevant.

Video-surveillance systems for security or other surveillance purposes should always be built using the principle of privacy by design and data protection

Video-surveillance must be used responsibly and with effective safeguards in place.

requirements should be an integral part of any such system development. Data processing systems should be designed and selected with the aim of minimising the collection and use of personal data. The designers of the system should also identify and make best use of available techniques. Data protection concerns should be addressed early on. The reasons for this are clear: once a system is in place, it is harder to include data protection friendly solutions, for instance, to guarantee the necessary levels of security, to give different levels of access and to ensure a reliable audit trail or the access rights of data subjects.

Accountability means that a responsible organisation (the controller) should be able to demonstrate compliance with its data protection obligations. This stimulates the use of data protection and privacy impact assessments and audits, and shifts the balance in privacy compliance from checks by regulatory authorities to proactive measures taken by the controllers themselves. The need to demonstrate compliance to stakeholders and regulatory authorities also means that accountability results in more transparency, for example making an organisation's video-surveillance policy public.

Standard systems versus increased scrutiny

The guidelines are designed to provide detailed data protection safeguards for most standard video-surveillance systems operated for common security purposes. Thus, in the majority of cases, there is no need to make a more formal and in-depth assessment of the data protection impact of an institution's video-surveillance, introduce new safeguards, or submit surveillance plans for prior checking by the EDPS. All that needs to be done is to follow and implement the guidelines.

However, when the proposed surveillance significantly increases the risks to the fundamental rights and legitimate interests of those under surveillance (compared with standard video-surveillance systems and safeguards described in the guidelines), a privacy and data protection impact assessment should be carried out before installing and implementing the system. The purpose of the impact assessment is to determine the additional impacts of the proposed system on an individual's privacy and other fundamental rights, and to identify ways to mitigate or avoid any adverse effects. These systems are subject to prior checking, and will be closely scrutinised by the EDPS.

Under close scrutiny:
- *employee monitoring, and monitoring individual offices;*
- *covert surveillance, and use of video-surveillance in investigations;*
- *monitoring demonstrators;*
- *high-tech or intelligent video-surveillance (e.g. face recognition, dynamic-preventive surveillance);*
- *interconnected systems;*
- *sound-recording and 'talking CCTV'.*

2.8. Eurodac

Eurodac was set up by Council Regulation (EC) No 2725/2000 (the so-called 'Eurodac regulation') which, together with the Dublin II regulation, is currently under review. Eurodac is a large database of the fingerprints of applicants for asylum and illegal immigrants in the European Union. The objective of the system is to facilitate the effective application of the Dublin II regulation which determines the EU Member State responsible for examination of an application for asylum by persons seeking international protection under the Geneva Convention within the European Union.

The EDPS is entrusted with the task of **supervising the processing of personal data in the central database of the system operated by the Commission** and their transmission to the Member States. Under this role, the EDPS cooperates closely with the data protection authorities in the Member States which supervise the processing of data at national levels, as well as the transmission of data to the central unit. The representatives of the data protection authorities and the EDPS meet regularly to discuss common problems relating to the functioning of the system.

This **coordinated supervision model** is a very successful example of a coordinated approach to data protection supervision (see Section 4.3).

The EDPS's activities in relation to Eurodac also involve consultation and advisory tasks performed in the context of the revision of the Eurodac and Dublin regulations currently under discussed by EU institutions. In February 2009, the EDPS issued two opinions on this matter (see Section 3.3.2).

3

CONSULTATION

3.1. Introduction: an overview, including some trends

A number of significant activities and events in 2009 helped bring **the prospect of a new legal framework for data protection** closer. Realising this prospect will be a dominant item on the EDPS's agenda over the coming years.

At the end of 2008, a general legal framework for data protection in the area of police and judicial cooperation was adopted at EU level for the first time (Council Framework Decision 2008/977/JHA). In 2009, a second major legislative development took place.

The first modernisation of the legal framework for data protection — the e-privacy directive (2002/58/EC) — was revised by Directive 2009/136/EC on 25 November 2009.

However, these are only the first steps.

The entry into force of the Lisbon Treaty marks a new era for data protection. Article 16 TFEU not only contains an individual right of the data subject, but it also obliges the European Parliament and Council to provide for data protection in all areas of EU law.

In other words, it allows for a comprehensive legal framework for data protection applicable to the private sector, the public sector in the Member States and the EU institutions and bodies.

The Stockholm programme — an open and secure Europe serving and protecting the citizen, as approved by the European Council in December 2009 — states that the Union must secure a comprehensive strategy to protect data within the EU and in its relations with other countries. In the EDPS opinion on the Stockholm programme, the need for a new legislative framework was emphasised, inter alia replacing Council Framework Decision 2008/977/JHA.

The most important step in this context is, however, the public consultation on the legal framework for the fundamental right to protection of personal data, organised by the Justice, Freedom and Security DG.

This public consultation must be seen as a first step towards a modern and comprehensive legal instrument for data protection that fully reflects the changes brought about by the Lisbon Treaty and will also ensure the effective protection of personal data in the information society.

The joint contribution of the Article 29 Working Party and the Working Party on Police and Justice on 'The future of privacy' was adopted in December

2009 with the full support and substantial contributions of the EDPS. This document should be given serious consideration as the relevant advice of the European data protection community for the development of the modern and comprehensive legal framework referred to above.

In the global context, it is important to note that the 31st International Conference of Data Protection and Privacy that was held in Madrid in November 2009 adopted a resolution on international standards in data protection. In relation to transatlantic data protection, further steps have been taken towards an agreement between the EU and the USA on the exchange of personal data for purposes relating to law enforcement.

The year 2009 can also be characterised as a year in which the EDPS got involved in two additional areas of EU policy in which the processing of personal data is of utmost importance: terrorists' lists and taxation.

The policy relating to so-called 'terrorists' lists' is part of the common foreign and security policy of the EU, and taxation is an area which by nature involves intensive personal data processing and administrative cooperation, notably to combat fraud. The focus on two other areas, namely public health and transport, was intensified. Finally, it goes without saying that the EDPS remained closely involved with various activities of the Information Society and Media DG and the Justice, Freedom and Security DG.

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 entitled 'The EDPS as an advisor to the Community institutions on proposals for legislation and related documents' ([8]) remains current, although it must now be read in light of the Lisbon Treaty.

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

Occasionally, comments are written for more limited purposes, to give a quick and fundamental political message or to focus on one or more technical aspects.

The EDPS is available during all phases of policy-making and legislation, and uses a wide range of other instruments for influencing. Although this may require close contact with EU institutions, safeguarding the EDPS's independence and respecting the position of all other institutions involved are paramount.

Contact with the Commission takes place in different stages of the preparation of proposals, and the intensity varies depending on the subject and also on the approach of the Commission services. For instance, in long-term projects, such as e-justice or the discussions on a framework for notification of security breaches, the EDPS contributed at different stages and in different ways.

Likewise, contacts in the follow-up phase took place, especially during intensive discussions and negotiations in Parliament or Council leading to fundamental amendments to a Commission proposal. Examples of intensive, multi-phased EDPS involvement in 2009 are the review of the e-privacy directive and the amendment of the public access regulation.

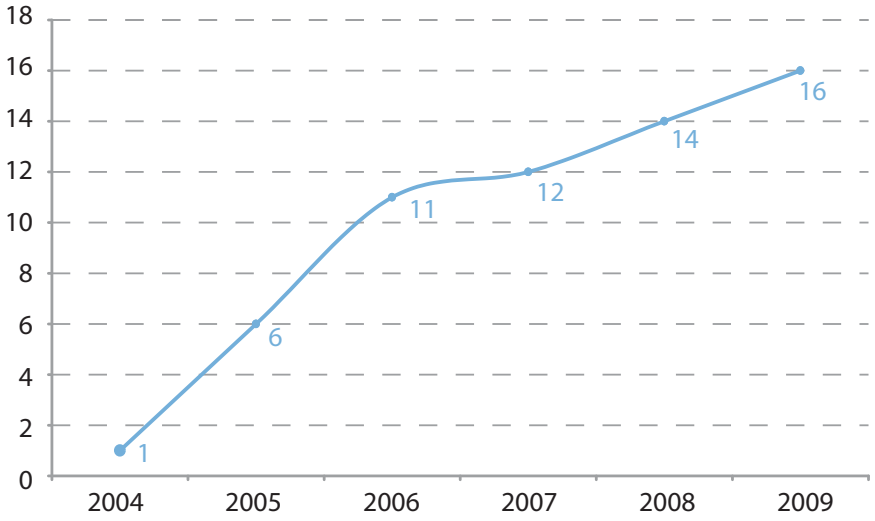
As stated earlier, in 2009, the possibility of a new framework for data protection became more concrete, and the subject was tabled at various levels and in various networks. The EDPS conveyed his message in a number of ways. Important landmarks were the opinion on the Stockholm programme and the report of the Article 29 Working Party, but other opinions — such as on law enforcement access to Eurodac — should be noted, along with speeches, contributions to conferences, and discussions in the European Parliament, etc. One of the key messages — namely that a comprehensive framework is needed, including police and judicial cooperation — was also presented by Commissioner Reding as one of her main objectives.

([8]) Available on the EDPS website, under Consultation section.

3.2.2. Results of 2009

In 2009, the steady increase in the number of consultative opinions continued. The EDPS issued 16 opinions on a wide variety of subjects.

Legislative opinions' evolution 2004–09

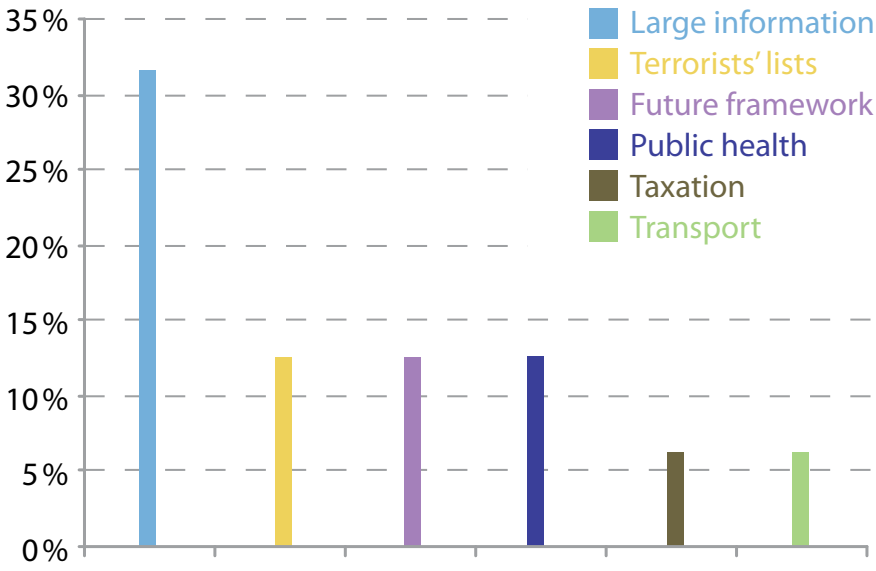


With these opinions, and the other instruments used for intervention, the EDPS implemented the priorities for 2009, as laid down in the inventory published in December 2008. The 16 opinions covered different EU policy areas.

The inventory for 2009 defined three main areas of attention, namely public health, freedom, security and justice, and the information society. Public health is a relatively new area for the EDPS: general positions were developed in the opinions on organ donation and pharmaco-vigilance. In the area of freedom, security and justice, much attention was given to developments relating to border management and large-scale information systems. The development of the information society was high on the agenda and will remain so.

In retrospect, whilst the EDPS focused on the main priorities of the 2009 inventory, the specific achievements of the year did not fully correspond with the intentions of the inventory. This shows the dynamics of this area. The issues that were identified at the beginning of the year did not always prove the most relevant during the year. However, the EDPS did not fundamentally alter his direction. Some plans, announced at the beginning of 2009, will lead to results in 2010. One example is an opinion delivered early 2010 on the Anti-Counterfeiting Trade Agreement (ACTA).

Main policy areas for legislative opinions in 2009



3.3. Area of freedom, security and justice

3.3.1. General developments

During 2009, the EDPS followed with particular interest the developments concerning the **Stockholm programme**, which puts forward the EU vision for the next five years in the area of justice and home affairs. The Stockholm programme must be seen as a further step in the construction of an area of freedom, security and justice in the European Union.

In this area, cooperation between law enforcement authorities and more generally between Member States, and between Member States and the EU, relies heavily on the collection and exchange of personal data. Protecting citizens' personal data in police and judicial cooperation is therefore crucial, as the EDPS has highlighted in more than 30 opinions and comments on this matter. The EDPS has consistently emphasised that ensuring the protection of personal data is not just a way of protecting citizens, but also a way of fostering efficient law enforcement and mutual trust between the law enforcement agencies of different Member States.

The EDPS issued an opinion on the Commission communication of 10 June 2009 and then actively contributed — through contributions and speeches delivered to relevant institutional stakeholders — to the debate leading to the adoption of the programme at the December meeting of the European Council.

The EDPS supported the attention that the programme devotes to the protection of fundamental rights, and in particular the protection of personal data. Likewise, the EDPS welcomes the call for a comprehensive data protection scheme, which now finds a solid legal basis in the Lisbon Treaty.

A comprehensive framework would also help to better address and regulate the most significant recent trends:

- *the exponential **growth of digital information** as a result of evolving information and communication technologies;*
- *the **internationalisation** of the exchanges of personal data;*
- *the **use of commercial data** for law enforcement purposes, e.g. data collected by private companies such as telecom operators, banks, airlines, etc.*

The EDPS stressed that EU institutions should reflect on the consequences for law enforcement authorities and for European citizens before adopting new exchange instruments. Furthermore, the EDPS highlighted the importance of developing and promoting international standards on data

The Stockholm programme states that the Union must secure a comprehensive strategy to protect data within the EU and in its relations with other countries.

protection, as well as of ensuring that personal data are transferred to third countries and organisations only when their adequate protection is ensured.

The Stockholm programme emphasises the project of a **European information model**, which represents a welcome effort to rationalise and develop a long-term vision for the management and exchange of personal data in the areas of justice, security, asylum and immigration.

The EDPS stressed that this long-term vision could be useful in building more effective exchanges of information while ensuring a high level of protection of personal data. Introducing privacy from the very beginning in the architecture of information systems — 'privacy by design' or 'privacy by default' — is a crucial step in implementing this long-term vision, since it will help enhance the quality of information and avoid information overload.

The EDPS also discussed the **interoperability** of different systems and databases, which should not be technology-driven, but based on clear and careful policy choices. It should respect and ensure legal conditions for the collection, exchange and use of personal data.

Citizens must be in a position to foresee which data about them are collected and for which purposes they are used. This is even more important when dealing with special categories of data such as fingerprints and DNA ([9]).

New technologies will also be used as a tool for **better judicial cooperation**, in the so-called **e-justice** project and other initiatives, to build a real European judicial area. Interconnection of national registers, such as insolvency registers, use of videoconferences in legal proceedings, and the use of Internet portals to enhance citizens' access to justice, are all elements of these initiatives, which the EDPS welcomes, provided data protection principles are embedded in their implementation. Some of these tools also can be used to facilitate more effective protection and easier Europe-wide enforcement of data protection rights.

([9]) As also follows from the conditions formulated by the European Court of Human Rights in the case *S. and Marper*, 4 December 2008, Appl. Nos 30562/04 and 30566/04.

3.3.2. Eurodac and Dublin regulation

Special attention should be paid to privacy and data protection issues in the Dublin system and Eurodac, the large-scale system for storage and exchange of digital fingerprints of asylum seekers and other groups of (potential) immigrants, which allows the determination of the Member State with responsibility for dealing with an application for asylum. The persons affected by this system are amongst the **most vulnerable in the population**, and face great difficulties when it comes to defending their rights.

Data protection is also a **key success factor** for the operation of Eurodac, and consequently for the proper functioning of the Dublin system. Elements such as data security, technical quality of data and lawfulness of consultation all contribute to the smooth functioning of the Eurodac system.

The EDPS adopted two interlinked opinions relating to the proposal for a revision of the so-called 'Eurodac regulation' and the proposal recasting the Dublin regulation which determines the EU Member State responsible for an asylum application.

These proposals aim to ensure a higher degree of harmonisation, increased efficiency and better standards of protection for the common European asylum system. They are also of special relevance to the EDPS given his current role as the supervisory authority of Eurodac.

In his opinions, the EDPS supported the objectives of the revision and welcomed the considerable attention which has been devoted in both proposals to the respect of fundamental rights of third-country nationals and stateless persons. The EDPS made a number of observations relating inter alia to the respect for the rights of the data subject, the supervision of the system and the mechanisms for information sharing.

The Commission also proposed allowing access to the Eurodac system — which is meant to facilitate the application of the Dublin regulation by comparing the fingerprints of asylum seekers and illegal immigrants — to law enforcement authorities for the prevention, detection and investigation of terrorist offences, and other serious offences under the conditions set out in the proposals.

The EDPS analysed the proposals in light of their proportionality and legitimacy, taking as a starting point the need to strike the right balance between the need for public security and the fundamental right to privacy and data protection, in compliance with Article 8 of the European Convention on Human Rights (ECHR).

The analysis led to the conclusion that the necessity and proportionality of the proposals, which are both crucial elements to legitimate privacy intrusion, had not been demonstrated.

The EDPS recommended assessing the legitimacy of the proposals in a wider context, notably:

- the tendency of granting law enforcement access to personal data of individuals that are not suspected of any crime and that have been collected for other purposes;
- the need for a case-by-case assessment of every proposal of this kind; and
- the need for a coherent, comprehensive and future-oriented vision, preferably related to the next five-year framework programme for justice and home affairs ('Stockholm programme').

3.3.3. Agency for the operational management of large-scale IT systems

The Commission has proposed a legislative package establishing an agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

The agency would be responsible for the operational management of the Schengen information system (SIS II), the visa information system (VIS), Eurodac and possibly other large-scale IT systems.

As these databases contain **large amounts of personal data** (e.g. details of passports, visas and fingerprints) some of which are of a sensitive nature, the EDPS analysed the proposal with a view to ensuring that the **impact on the privacy of individuals** is sufficiently addressed in the legislative instrument.

The EDPS sees the advantages of setting up an agency for the operational management of certain large-scale IT systems, but such an agency should only be established if the scope of its activities and responsibilities are clearly defined.

The creation of an agency for the operational management of large-scale databases must be based on legislation which is unambiguous regarding the competences and the scope of activities of the agency. Such clarity would prevent any future misunderstanding about the conduct of the agency and avoid the risk of function creep. As currently drafted, the proposals do not meet these requirements.

3.3.4. Customs information system (CIS)

A **coherent and comprehensive approach to EU large-scale IT systems** as well as **efficient data protection supervision** are essential elements for the success of the operations of these systems. The new legal framework provided by the Lisbon Treaty and the abolition of the pillar structure of EU law should also serve as a tool to provide more **coherence** between the systems formerly based on the first and third pillar legal basis. There is also a need for increased collaboration between the data protection bodies involved in the supervision of the systems.

Against this background, the EDPS issued an opinion on the initiative of the French Republic for a Council decision on the use of information technology for customs purposes. In this opinion, the EDPS stressed the need to ensure as much coherence as possible between the two parts of the CIS, i.e. the part governed by the former first pillar and the part governed by the former third pillar. The EDPS called for more attention to be devoted within the proposal to **specific data protection safeguards**, particularly with respect to purpose limitation for the use of data entered in the CIS.

The EDPS also called for a **coordinated model of supervision** to be inserted into the proposal, which would ensure, where necessary, consistency with other legal instruments governing the establishment and/or use of other large-scale IT systems, since this model is also anticipated for SIS II and VIS.

The model of supervision was a significant topic in the discussions in Council and the European Parliament. The EDPS invested much time and energy in pleading for a coordinated model. Unfortunately, the Council adopted a text which does not fully reflect this model. On the other hand, the text does give a greater impetus to close and effective cooperation between the EDPS and national data protection authorities.

3.4. E-privacy and technology

3.4.1. EDPS and e-privacy directive

During 2009, Directive 2002/58/EC on privacy and electronic communications, also known as the **e-privacy directive**, underwent the final steps of the review process. Final adoption took place on 25 November 2009 ([10]). Its new provisions strengthen the protection of the privacy and personal data of all Europeans active in the online environment. Particularly relevant improvements include:

- mandatory notification of personal data breaches. Any provider of electronic communications services such as an Internet service provider must inform individuals of any personal data breaches likely to adversely affect them; examples include those where the loss of personal data could result in identity theft, fraud, humiliation or damage to reputation;
- new regulations on cookies and spyware; under the new provision, users should be offered better information and easier ways to accept or reject cookies being stored on their terminal equipment;
- enhancement of the right of action against spammers; this is achieved by giving any person negatively affected by spam, including ISPs, the possibility to bring effective legal proceedings against the spammers;
- provisions strengthening the enforcement powers for data protection authorities.

Throughout the legislative process until its final adoption, the EDPS remained fully available to policy-makers to advise and assist them in defining the appropriate policy solutions. The EDPS was particularly pleased with the final framework on mandatory security breach notification.

In his second legislative opinion, the EDPS advised, among other things, on the main features of the legal framework on security breach notification ([11]).

The EDPS welcomed the broad definition of security breach including any breach leading to the destruction, loss, disclosure, etc. of personal data transmitted, stored or otherwise processed in connection with the service. As a trigger or standard for notification, he suggested that notification to individuals should be required if the data breach is *likely to adversely affect their personal data or privacy*. He gave reasons why this standard was preferable to other proposed standards and was pleased when his preference was followed. He also welcomed the decision to make the entities concerned responsible for the assessment of whether the breach met or failed to meet the standard or trigger.

Unfortunately, the legislator did not follow the EDPS recommendation to make this provision applicable to all data controllers, and rather chose to limit it to electronic communications services, such as telecommunication companies, Internet service providers, webmail providers, etc.

This limitation of the scope triggered a heated debate between the European Parliament — favouring a substantially broader scope — and the Council and Commission supporting a more limited scope. Whilst the final outcome is unsatisfactory, the debate caused the Commission to express its

([10]) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ L 337, 18.12.2009, p. 11).

([11]) Second opinion of 9 January 2009 on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications) (OJ C 128, 6.6.2009, p. 28).

Electronic communications always leave traces of individuals.

intention to make this regime mandatory for all data controllers in the near future.

The revised e-privacy directive empowers the Commission in consultation with stakeholders and the EDPS to adopt technical implementing measures, i.e. detailed measures on security breach notification, through a comitology procedure. This will ensure consistent implementation and application of the security breach legal framework across the EU, so that citizens enjoy an equally high level of protection and service providers are not burdened with diverging notification requirements.

The EDPS organised two events to share experience and best practice. These initiatives should be helpful in the future comitology procedure. The first event took place in April 2009. It was organised under the umbrella of the 'London initiative' for data protection authorities only. The second event with a general stakeholder audience took place in October 2009 and was jointly organised with the European Network and Information Security Agency (ENISA).

The e-privacy directive was adopted together with other directives, referred to collectively as the **telecoms package**.

The provisions on graduated response schemes or the so-called 'three strikes approach', included in Directive 2002/22/EC on universal service and users' rights, raised data protection and privacy issues. The EDPS addressed these in comments of 16 February 2009, confirming his views against the systematic, proactive surveillance of law-abiding Internet users to fight alleged copyright infringements.

3.4.2. Intelligent transport systems

The EDPS has drawn particular attention to technological innovation in the field of transport. So-called 'intelligent transport systems' (ITS) are currently being deployed in Europe, with the aim of reducing traffic congestion and making transport safer and cleaner. The systems usually rely upon location technologies, such as satellite-based localisation and RFID. The deployment of ITS in Europe has considerable privacy implications, notably because they make it possible to track a vehicle and to collect a wide variety of data relating to European road users' driving habits.

'Intelligent transport systems' apply information and communication technologies (such as satellite, computer, telephone, etc.) to transport infrastructure and vehicles. The emergency call system 'e-Call' and the electronic tolling system 'e-Toll' are examples of intelligent transport systems.

Commenting on a Commission action plan to accelerate and coordinate the deployment of ITS in Europe, the EDPS stressed the need to carefully address privacy and data protection issues in order to ensure the workability of ITS across Europe.

He further warned the Commission about the risks of inconsistencies and fragmentation in such deployment if certain issues are not further harmonised at EU level.

Modern technology makes it possible to continuously monitor the movement of drivers.

- There is a need to clarify whether, and if so which, ITS services will be provided on either a voluntary or a mandatory basis.

- It is crucial to clarify the roles of the different parties involved in ITS in order to identify who has responsibility for ensuring that the systems work properly from a data protection perspective — i.e. who is the data controller?

- Appropriate safeguards should be implemented by data controllers providing ITS services so that the use of location technologies is not privacy intrusive. The use of location devices should be strictly limited to what is necessary for their purpose. It should be ensured that location data are not disclosed to unauthorised recipients.

- Privacy and data protection should be considered at an early stage in the design of ITS architecture, operation and management of the systems ('privacy by design').

- Data controllers must ensure that users are appropriately informed about the purposes and manner in which the data processing takes place.

3.4.3. Application of the data retention directive

The data retention directive (2006/24/EC) is an instrument for the combat of terrorism and other serious criminal offences, which obliges providers of communications services and networks to retain the traffic data of electronic communications. It was adopted a few years ago, under intense political pressure, and raises many questions which make its application difficult.

An expert group bringing together the interests of law enforcement, industry and the data subject was therefore established with the main task of providing guidance — for example on the issue as to which providers does the directive apply, given the complex environment of webmail services, transit providers, third party networks, etc. The EDPS actively participated in this group and insisted that any guidance conforms to the principles of data protection law.

In this context, an interesting and difficult question arose, namely what law applies in case of communications which involve more than one Member State, for instance in the case of international mobile communications or cross-border Internet communications. This issue becomes even more complex where the provider stores the retained data in a Member State other than the one in which

they were generated. The group intends to publish its conclusions in the course of 2010.

3.4.4. RFID

In May 2009, the European Commission adopted a recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification ([12]). The EDPS was frequently consulted by the Commission during the preparation of the recommendation and the majority of his comments have been introduced.

The European Commission then set up an informal working group on the implementation of the RFID recommendation and a representative of the Article 29 Working Party (WP29) attended the two meetings of the group in 2009. Topics addressed by the group included the need for a privacy and data protection impact assessment (PIA). According to point 4 of the recommendation, a PIA framework will be submitted to the WP29 for its endorsement.

3.4.5. Involvement in FP7

RISEPTIS

The EDPS joined the Advisory Board RISEPTIS (research and innovation for security, privacy and trustworthiness in the information society) ([13]) as an observer. This high-level advisory group established by the European Commission and composed of leading scientific, industrial and policy stakeholders aimed to provide visionary guidance on policy and research challenges in the field of security and trust in the information society. The EDPS took an active role in the RISEPTIS meetings held in 2009, and provided targeted policy advice, notably on the issues of applicable law for future and emerging technologies, the principles of accountability and liability, as well as the concept of privacy by design.

The RISEPTIS report entitled 'Trust in the information society' and issued in October 2009, contains recommendations to address a number of issues as the EU moves forward into the digital age.

([12]) Commission recommendation C(2009) 3200 final of 12 May 2009 (available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf).

([13]) http://www.think-trust.eu/riseptis.html

These include:

- interdisciplinary research, technology development and deployment;
- initiatives to bring together technology, policy, legal and socioeconomic stakeholders to work towards a trustworthy information society;
- a common EU framework for identity and authentication management;
- further development of the EU data protection and privacy legal framework;
- large-scale activities involving the private and public sector, which take advantage of Europe's strengths in communication, research, legal studies and societal values;
- cooperation on a global scale to promote open standards and federated frameworks.

EU RTD projects

Following his policy paper of May 2008, the EDPS also provided targeted support and feedback to a series of EU RTD projects in various fields, including intelligent transport systems, biometrics, remote monitoring systems, and e-health.

3.5. Globalisation

3.5.1. Involvement in global standards

Many stakeholders including civil society and industry argue for a harmonised data protection framework across borders, in order to ensure legal certainty and facilitate data flows in an international context. Concrete steps towards developing international data protection standards were taken at the International Conference of Data Protection Commissioners held in Madrid in November 2009. The conference adopted a resolution welcoming draft 'International standards on the protection of personal data and privacy'. These standards represent the first step towards a binding international instrument. They are the result of intensive preparatory work led by the Spanish data protection authority, in which the EDPS has also taken an active part.

The standards include the core principles of data protection and, whilst these principles are to a large extent inspired by the European data protection directive, they also take other approaches to data protection ([14]) into account.

Compliance with the fairness, necessity, proportionality and transparency principles is complemented with accountability obligations for data controllers, as well as the need to integrate privacy by design. The draft standards also provide access and rectification rights to data subjects, as well as judicial and administrative redress.

3.5.2. PNR and transatlantic dialogue

Data protection issues are high on the agenda of the talks between the EU and the USA.

Another aspect of globalisation is the transatlantic dialogue between the European Union and the United States to facilitate the exchange of personal data. Transfers of data take place mostly for the purposes of fighting terrorism and serious crimes, as shown by the agreement on the transfer of passenger data to the Department of Homeland Security of the United States (Council decision of 23 July 2007). Both the Article 29 Working Party and the EDPS have expressed concerns about the conditions under which passenger data are collected, processed and stored ([15]). In 2009 a subgroup of the WP29 in which the EDPS participates monitored the implementation of this PNR agreement and raised a number of issues, notably the wide access given to the US administration to data processed by computer reservation systems, and the absence of review of the system by European authorities.

In a wider context, the EU and the USA are negotiating the conclusion of an agreement on information sharing in the broad area of law enforcement. Negotiations have led to several reports from the so-called High Level Contact Group, on which the EDPS has issued an opinion ([16]). In 2009, discussions focused on specific issues where there was no full agreement between the parties, and in particular on the right for individuals to administrative *and* judicial redress. The parties intend to make further steps towards an agreement in the course of 2010. The EDPS has provided input to the public consultation on the agreement, organised by the Commission.

([14]) Such as the approach of the OECD and APEC countries, which differs slightly from that of the EU.

([15]) See EDPS Annual Report 2008.

([16]) Opinion of 11 November 2008 on the Final Report by the EU–US High Level Contact Group on information sharing and privacy and personal data protection (OJ C 128, 6.6.2009, p. 1).

Access by public authorities to bank transactions' data shall be subject to stringent conditions.

3.5.3. SWIFT: transfer of financial data to US authorities

The EDPS closely followed developments concerning the transfer of European financial transaction data to the US Treasury for the purposes of combating terrorism and terrorism financing. This is a clear example of personal data collected by commercial companies, which are used for the purposes of global law enforcement.

When SWIFT, the major financial data carrier, changed its architecture in order to keep European financial data in European territory, the European Commission started negotiating an international agreement with US authorities in order to avoid discontinuing their access to these data. The EDPS was consulted and issued some comments, which were sent to relevant institutions and presented to the LIBE Committee in September 2009.

An interim agreement was signed in November 2009, but under the new rules of the Lisbon Treaty the European Parliament withheld its consent. During 2010, the EDPS will continue to advise EU institutions to ensure that European standards for the protection of personal data are upheld, particularly in relation to any new agreement that will replace the interim agreement.

According to the EDPS, an international agreement should ensure that:

- *the requests for data transfers are lawful and proportionate, particularly in light of the privacy-intrusive nature of the proposal;*
- *redress mechanisms are available and can be used effectively by European citizens;*
- *further sharing with other national authorities and other countries is limited;*
- *independent data protection supervisory authorities can exercise their supervisory powers including a review of the implementation of the agreement.*

3.5.4. Restrictive measures with regard to suspected terrorists and certain third countries

In two opinions in 2009, the EDPS addressed so-called 'terrorist blacklists' for the first time. These legal instruments envisage fighting terrorism or human rights abuses by imposing restrictive measures — notably asset-freezing and travel bans — on natural and legal persons suspected of being associated with terrorist organisations and/or certain governments. The European Commission publishes and publicises 'blacklists' of persons who are subject to these restrictive measures.

In several cases the Court of Justice reaffirmed that all EU measures, even those stemming from UN decisions, should respect EU fundamental rights, in particular the right to a defence and the right to be heard. Notably, the Court annulled the listing of certain individuals either because they were not in a position to know the reason for their listing, or they had remained on the list for several years without any formal conviction or actual ongoing investigation.

The EDPS welcomed the more recent Commission proposals aimed at improving the respect of fundamental rights and explicitly recognising the applicability of Regulation (EC) No 45/2001 to this politically sensitive area.

He recommended that:

- data quality be ensured, by taking into account relevant developments in the police and security enquiries on which listings are based, and by carrying out regular reviews of the lists;
- listed persons be provided with adequate information and with the right to have access to personal data concerning them;
- necessary restrictions and limitations to these rights be clearly laid down in law, and be anticipated and proportionate;
- judicial remedies, liability and adequate compensation be ensured in case of the unlawful processing of personal data.

The EDPS will continue to follow developments in this area both as an advisor to the EU institutions and as the supervisor of the processing of these blacklists, which was notified for prior checking by the European Commission at the end of 2009.

The EDPS was for the first time actively involved in this sensitive area.

Must personal data be processed in the EudraVigilance database?

3.6. Public health

The EU has an ambitious programme for improving citizens' health in the information society and sees great possibilities for enhancing cross-border healthcare through the use of information technology. It is, however, obvious that enhancing cross-border healthcare through the use of information technology has significant implications for the protection of personal data.

Since 2008, concrete initiatives in this area were adopted or proposed by the Commission. The Commission published a communication on telemedicine and a recommendation on cross-border interoperability of electronic health record systems. It also improved the early warning and response system in relation to communicable diseases and proposed legislation on patients' rights in cross-border healthcare, organ transplantation and pharmaco-vigilance (detection and analysis of the adverse effects of medicines).

The EDPS expressed a general concern that most of these texts pay only lip service to data protection. The issue of data protection is mentioned and reference is made to applicable data protection law, but no concrete rules are proposed which actually ensure compliance with data protection requirements and ensure that Member States apply these rules in a consistent manner. A coherent vision of data protection in the healthcare sector seems to be absent.

This can be partly explained by the lack of awareness of data protection within the public health sector, as reflected at EU level by the lack of awareness in responsible departments of the EDPS' existence and the duty to consult him. The most striking example in this respect was the proposal on pharmaco-vigilance which made almost no mention of data protection and was not sent to the EDPS for consultation.

The EDPS repeatedly emphasised that health data are considered a sensitive category of personal information and that the processing of such data is in principle prohibited. There are exceptions, for instance when someone is subject to a medical diagnosis, but these exceptions must be applied restrictively.

In the opinion on pharmaco-vigilance, the EDPS highlighted the necessity principle, and questioned the need for processing personal data in the centralised European EudraVigilance database.

In the opinion on organ transplantation, the EDPS clarified the concept of 'anonymisation'. He explained that if the traceability of organs is ensured, which means that the donor can always be traced, the accompanying information can never be considered anonymous. Since the proposals ensured the traceability and anonymity of information at the same time, they had to be adjusted by putting emphasis on the confidentiality of information instead of its anonymity.

The EDPS has repeatedly emphasised that data protection rules are not put into place to obstruct effi-

cient cooperation in the field of public health. On the contrary, data protection safeguards are crucial for preserving confidence in the medical profession and health services in general.

The European Court of Human Rights has ruled that 'the protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention'. And: 'respecting the confidentiality of health data is [...] crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general' ([17]).

The EDPS welcomed invitations from the ENVI Committee of the European Parliament which enabled him to explain two of his opinions (on cross-border healthcare and organ transplantation). The EDPS was also pleased that his suggestions led to several amendments being adopted by the European Parliament, although as yet none of the proposed legal instruments themselves have been adopted.

The consultation on the proposals relating to pharmaco-vigilance was combined with an analysis on the basis of a prior-check notification of the system by the European Medicines Agency (EMA). The same was true for the further development of the early warning and response system in relation to communicable diseases by the Commission and the European Centre for Disease Prevention and Control (ECDC). The EDPS provided informal comments on the relevant Commission decision and started an analysis of the system after receiving a notification for a prior check.

Activities in the area of public health have led the EDPS to take an integrated approach with regard to his consultative and supervisory roles.

([17]) See European Court of Human Rights, 17 July 2008, *I* v *Finland* (Appl. No 20511/03), paragraph 38.

3.7. Public access and personal data

3.7.1. Introduction

The complex relationship between EU rules on public access to documents and data protection has concerned the EDPS for several years. In 2009, the EDPS participated in the discussion on the modification of the EU legislation on public access to documents, and intervened in Court cases on the matter, including the *Bavarian Lager* case. In addition, the first case brought before the General Court against an EDPS decision on a complaint dealt with this subject.

3.7.2. Modification of EU legislation on public access to documents

Having noted the developing discussions in the European Parliament concerning the modification of the EU legislation on public access to documents, the EDPS summarised the views expressed in his opinion of 30 June 2008 into brief comments. The EDPS highlighted the negative consequences of some of the amendments tabled in Parliament for the relationship between both rights. The EDPS was pleased that the outcome of the votes in the plenary session almost completely reflected his approach.

In a press release issued after the vote, the EDPS stated: 'These amendments create clarity and prevent an overzealous application of data protection rules in this area. They confirm that data protection does not stand in the way of public disclosure of personal information in cases where the person involved has no legitimate reason for keeping the data secret.'

The EDPS gave an oral explanation of his views in the Council Working Party on Information. Despite the efforts of the Swedish Presidency to push the modification through Council in the second half of 2009, the discussion on the modification stagnated because of a procedural conflict between the Commission and the Parliament, a conflict which is as yet unresolved.

3.7.3. The appeal in the *Bavarian Lager* case

The *Bavarian Lager* case concerned the refusal of the Commission to disclose five names contained in a Commission document. The judgment of the General Court of 8 November 2007 was appealed by the Commission and led to a Court hearing on 16 June 2009. During this hearing the EDPS pleaded in favour of upholding the judgment of the General Court. Although Advocate General Sharpston in her opinion of 15 October 2009 also dismissed the appeal of the Commission, she did not share the reasoning of the General Court as supported by the EDPS. Since the conclusion drawn by the Advocate General was based on a reasoning which was not discussed between the parties at all, the EDPS and the Commission requested that the Court reopen the oral procedure.

3.7.4. Other Court cases on public access and data protection

The *Dennekamp* case before the General Court concerned the Parliament's refusal to disclose documents which show which Members of the European Parliament are also members of the Additional Pension Scheme. From a legal point of view the case can be seen as a specification of the *Bavarian Lager* case. For this reason, the EDPS intervened in the case.

The first ever case against an EDPS decision was instigated by Ms Kitou on 3 April 2009. She disagreed with a decision of the EDPS in which he concluded that data protection rules would not stand in the way of a public disclosure by the Commission of whether or not she was working at the Commission at given times.

Both cases are still pending as this Annual Report goes to print.

Two other relevant Court cases, which are also still pending, are those instigated by Mr Pachtitis against the Commission and EPSO, before both the General Court and the Civil Service Tribunal (CST). The subject matter of these cases differs from those described above since the applicant wanted access to his *own* personal data, which the Commission refused on the basis of the EU legislation on public access to documents. In the written pleadings and during the hearing before the CST, which took place on 1 December 2009, the EDPS argued that the request for access should have been considered under the data protection rules and that those rules should have been applied proactively by the Commission.

In the discussion on the modification of the EU rules on public access to documents, the EDPS argued that this obligation should be included in the preamble of the modified document. This suggestion was supported by the European Parliament.

The complex relationship between these two fundamental rights keeps the EDPS busy.

3.8. A variety of other issues

3.8.1. Internal market information system (IMI)

In 2009, the EDPS continued to be closely involved in the development of the IMI, possibly the most striking example of administrative cooperation through information sharing, and an instrument for further European integration. The IMI system became operational — over 4 500 competent authorities were registered to use IMI by the end of 2009 — and many steps have been taken to build data protection safeguards into the system.

The EDPS welcomed these efforts, but at the same time consistently underlined the importance of a more comprehensive framework for the operation of IMI to provide for legal certainty and a higher level of data protection — preferably a Council and Parliament regulation.

The information society becomes fully intertwined with the physical world of the individual.

3.8.2. Other opinions

The EDPS also produced some opinions on subjects in which data protection was not the central issue, although there was nevertheless a connection with the processing of personal data. These concerned: a proposal for a Council directive imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products; a proposal for a Council regulation establishing a Community control system for ensuring compliance with the rules of the common fisheries policy; and a recommendation for a Council regulation concerning the collection of statistical information by the European Central Bank.

3.9. A look into the future

3.9.1. Technology developments

As mentioned in the EDPS Annual Report for 2007, the information society should no longer be considered as a parallel and virtual environment but increasingly as a complex and interactive world intertwined with the physical world of the individual. The convergence of these two worlds is facilitated by the ever-increasing number of bridges created by the innovative use of existing technologies and the development of new and emerging technologies. This trend is natural and positive, and will ultimately lead to a full integration in which the information society will simply be part of society.

However, the proliferation of these bridges tends to blur the borders between environments which may not currently be governed by the same legal framework, and therefore creates legal uncertainties which can undermine trust and be detrimental to the development of the information society.

The examples in the box below illustrate some of these bridges.

- *'**Smart' CCTV:** Such systems are often used for investigating incidents which took place in the past and the subsequent prosecution of related offences. Coupled with face recognition software and linked to private or public databases such as social networks, real-time CCTV footage (the real world) could be enriched by additional online data (the digital world).*
- ***Internet of things:** This umbrella concept is defined in the communication of the Commission ([18]) issued in June 2009. These networks of interconnected tagged objects will obviously establish links between the physical nature of such objects (e.g. their location, situation, activities, behaviour, ownership) and the online information related to them, which is continuously fed by a network of sensors. In this new environment, the long lifecycle of some tagged objects (e.g. tyres, glasses) will consolidate the links, providing over time even more accurate information on both the objects and their owners.*

([18]) 'Internet of things — An action plan for Europe', COM(2009) 278 final of 18 June 2009 (http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf).

- ***The intelligent fridge:*** *This over-used example links home and kitchen appliances with online providers. Even if proactive monitoring of the usage of the fridge in the house is considered unacceptable, the processing of the data generated by the same fridge and communicated to online providers may be governed by different applicable laws.*
- ***Online behavioural advertising:*** *Processing and correlating a wide variety of data related to the online behaviour of individuals produces accurate profiles which can be used to tailor ads to each individual. Web browsers and/or new communication devices provide location data and movement patterns associated with other devices, objects, people, shops, etc., which, added to their online behaviour data, can help complete the user profiles.*

The convergence of these two worlds into a seamless space for the individual is undoubtedly creating new challenges for the EU privacy and data protection legal framework. The objective is of course to clearly reconcile the online and offline environments under a single harmonised umbrella or at least an enhanced interoperability between them, in order not to jeopardise trust in this promising digital age.

3.9.2. Policy and legislation developments

As this Annual Report goes to print important developments are taking place (or have taken place) which will determine the context for policy and legislation in 2010.

These developments will obviously become more tangible when the new Commission details its ambitions. The new Commission legislative and work programme for 2010 and the action plan for the implementation of the Stockholm programme will be important documents in this regard. The EDPS is, of course, particularly interested in the follow-up to the public consultation on the future framework for data protection.

Other areas where new developments are expected to have an impact on the processing of personal data include various European instruments in the areas of public health, cooperation in taxation, transport (including new developments relating to the monitoring of cars) and the e-justice project.

3.9.3. Priorities for 2010

The EDPS will establish his priorities for 2010 in the specific context of developments in the year and will continue the direction of his advisory policy from 2009. The priorities will be laid down in the 2010 inventor, which will be published following the Commission's legislative and work programme for 2010, now anticipated at the end of March 2010.

- *Most importantly, the **Lisbon Treaty** entered into force, strengthening the importance of data protection within the Treaty framework and requiring legislative action.*
- *The **Stockholm programme** puts significant emphasis on data protection. It highlights the importance of the protection of fundamental rights in the information society, and it stipulates data protection as a prerequisite to the exchange of information for the purpose of safeguarding the security of society.*
- *A **new Commission** began its work with high ambitions for data protection and privacy. The new Commissioner for Fundamental Rights and Justice continues to mention a comprehensive framework for data protection as one of her top priorities.*
- *The new Commission is working on **Europe's Digital Agenda**, in which **privacy and data protection are necessary preconditions**, with a strong emphasis on, for instance, privacy by design.*
- *There are also important developments which will allow the EU and its Member States to deal more effectively with the **external dimension of data protection**, not only in relation to the United States, as the most important stakeholder in data exchange, but also on a wider scale through the further development of global standards.*

4

COOPERATION

4.1. Article 29 Working Party

The Article 29 Working Party was established by Article 29 of Directive 95/46/EC. It is an independent advisory body on the protection of personal data within the scope of this directive ([19]). Its tasks are laid down in Article 30 of the directive and can be summarised as follows:

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

The EDPS has been a member of the Article 29 Working Party since early 2004. Article 46(g) of Regulation (EC) No 45/2001 provides that the EDPS participates in the activities of the working party. The EDPS 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 2009 the working party focused its activities on the items identified in its 2008–09 work programme, notably:

- better implementation of Directive 95/46/EC;
- ensuring data protection in international transfers;
- ensuring data protection in relation to new technologies;
- making the Article 29 Working Party more effective.

([19]) The working party is composed of representatives of the national supervisory authorities in each Member State, a representative of the authority established for the Community 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.

The working party adopted several documents in this regard, among which are:

- **Better implementation of Directive 95/46/EC:** Joint contribution on the 'future of privacy', in reply to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168);
- **International transfers:** Opinion 3/2009 on the draft Commission decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) (WP161); opinions on the adequacy of Andorra (WP166) and Israel (WP165);
- **New technologies:** Opinion on online social networking (WP163); opinion on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-privacy directive) (WP159).

The working party reacted to developments in the field of **new technologies**, and followed the implementation of its opinion on **search engines** adopted in 2008 by organising a hearing of search engine service providers.

The working party and the EDPS cooperated closely on issues related to new challenges in the field of data protection. In addition to close collaboration with regard to the **future of the data protection framework**, the working party and the EDPS drafted a common reply to the consultation of the Commission on 'the **impact of the use of body scanners** in the field of aviation security on human rights, privacy, personal dignity, health and data protection'.

The EDPS also cooperates with national supervisory authorities to the extent necessary for the performance of their duties, in particular by exchanging all useful information and requesting or delivering assistance in the execution 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 growing even more relevant in the context of the development of large international systems such as Eurodac, which require a coordinated approach to supervision (see Section 4.3).

4.2. Council Working Party on Data Protection

In recent years, under different presidencies, the Council Working Party on Data Protection has provided an opportunity for Member States to discuss data protection matters in the now former 'first pillar'. In 2009, the working party was convened only once, under the Czech Presidency. The EDPS used the occasion to give the representatives of the Member States an overview of his activities.

Due to an absence of general legislative initiatives on data protection in this area, the working party has not been able to fully reach its potential. However, by acting as an information-sharing platform and proactively offering its expertise, the working party could play a constructive role in helping to develop a comprehensive legal framework for data protection — a role the EDPS would welcome.

The Spanish Presidency has once again provided for a meeting of the working party in March 2010.

4.3. Coordinated supervision of Eurodac

The effective supervision of Eurodac relies on close cooperation between national data protection authorities and the EDPS. The Eurodac Supervision Coordination Group, composed of representatives of the national data protection authorities and the EDPS, met three times in 2009.

Second inspection report

One of the group's most significant achievements of this year was the adoption in June of its second inspection report. The report presents both the findings and recommendations based on the replies received from all the Member States. One of the aims of this exercise is to contribute effectively to the ongoing revision of the Eurodac and Dublin framework (see also Section 3.3.2).

The two main issues that were scrutinised by the group were: the right to information for asylum seekers and the methods for assessing the age of young asylum seekers. The report has been sent to the main EU institutional stakeholders, as well

as international organisations and NGOs dealing with asylum and immigration matters.

The right to information

Without clear and accessible information, the individuals subjected to the Eurodac system are unable to exercise their data protection rights.

The inspection showed that the information provided to asylum seekers about their rights and the use of their data tends to be incomplete, particularly the consequences of being fingerprinted, and the right of access to and rectification of their data. The information provided varies widely among Member States and significant differences have been observed in relation to the practices for asylum seekers and illegal immigrants.

Consequently, the report recommended that Member States should improve the quality of the information that they provide on data protection. This information should cover the rights of access and rectification as well as the procedure to exercise those rights. In addition, asylum authorities should ensure that the information is provided consistently to both asylum seekers and illegal aliens, and is clear and easily understandable. Particular emphasis should be placed on ensuring the visibility and accessibility of the information. Furthermore, Member States should promote cooperation and the sharing of experience between competent national authorities, by encouraging a working group to study this matter and eventually develop harmonised practices.

Assessment of the age of asylum seekers

The Eurodac regulation stipulates that children of 14 years and older should be fingerprinted. There is, however, often a problem in determining the age of a child who carries no reliable identity document, and therefore various methods are used at national level.

The inspection carried out by the group focused both on the methods for assessing the age of asylum seekers (involving intrusive medical examinations) and on the procedure surrounding the tests.

One of the conclusions was that the methods for determining the age of asylum seekers should be stated clearly and made accessible to the public.

It was suggested that, in order to promote harmonisation, the Commission should undertake an overall assessment (including medical and ethical aspects) of the reliability of the various methods of age assessment used in the Member States.

Furthermore, the asylum seeker should be entitled to ask for a second opinion regarding the medical results and the conclusions drawn from them without incurring costs. Asylum authorities have to take account of the margin of error resulting from the use of some medical examinations when taking decisions affecting the legal status of the asylum seeker.

4.4. Third pillar

The EDPS continued to cooperate with the joint supervisory bodies (JSBs) which deal with Schengen, Europol, Eurojust and the customs information system, and the Working Party on Police and Justice (WPPJ) set up by the European Conference of Data Protection Commissioners to monitor and act on developments in data protection in the area of law enforcement.

Work with the JSBs focused on exchanging information, and fostering consistency and improvements in data protection supervision, particularly in view of the entry into force of the Lisbon Treaty. The WPPJ can be considered as an informal complement of the Article 29 Working Party for areas where the latter is not competent, particularly the former 'third pillar'. As member of the WPPJ, the EDPS actively took part in its activities, including:

- contributing to the debate on the Stockholm programme;
- evaluating the impact of the Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation, focusing in particular on ways to guarantee a harmonised approach to implementation at national level;
- monitoring the implementation of the Council of Europe's Cybercrime Convention, the first international treaty defining a common policy for protecting society against crimes committed via the Internet or other computer networks;

- expressing deep concern, in accordance with the EDPS's opinion, about the Commission's proposal to allow access to Eurodac for law enforcement purposes;

- compiling a register of cooperation and supervision in the area of law enforcement in the EU, which was then adopted by the European conference;

- monitoring and improving the existing bilateral and multi-lateral agreements between European and non-European countries in the field of police and judicial cooperation in criminal matters, including the fight against terrorism;

- following the developments as to the international agreement with the USA on the transfer of financial messaging data for the purposes of the Terrorist Finance Tracking Program, as well as the broader debate on establishing transatlantic data protection principles;

- contributing to a joint paper on the future of data protection in Europe, in response to a public consultation launched by the European Commission.

To ensure consistency amongst the European data protection authorities, the WPPJ worked closely with the Article 29 Working Party and referred to the positions adopted by the EDPS.

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 Edinburgh on 23 and 24 April 2009.**

This conference focused on the need for a **review of the European data protection** framework. Four sessions were organised around this theme, including:

- the presentation of a draft report by RAND Europe, commissioned by the UK Information Commissioner's Office, entitled 'Review of the EU data protection directive', which was commented upon by the EDPS;

- 'Do we need reform at all? Other views of the strengths and weaknesses of Directive 95/46/EC';

- 'What outcomes should regulation achieve for individuals, society and regulators?';

- 'The international context of regulation'.

A declaration 'on leadership and the future of data protection in Europe' was adopted by the conference, highlighting the role of data protection authorities in this debate. The conference also adopted a resolution on bilateral agreements between EU Member States and third countries in the area of police and judicial cooperation in criminal matters.

The conference was also the occasion to report on the bi-annual meetings of the Case Handling Workshop, in which staff members from European data protection authorities participate with a view to exchanging best practice ideas. The workshops in 2009 were held in Prague (Czech Republic) and Limassol (Cyprus). The next case handling workshop will be held in Brussels in spring 2010.

The next European conference will be hosted by the Czech data protection authority in Prague on 29 and 30 April 2010.

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 Spanish data protection authority in Madrid on 4–6 November 2009**, attracting well over a thousand participants, more than ever before. Its main theme was 'Privacy: today is tomorrow'.

Several plenary sessions were organised to discuss the following issues:

- a society under surveillance? Striving for a balance between security and privacy;

Peter Hustinx speaking at the International Conference of Data Protection Commissioners (Madrid, 4–6 November 2009).

- *quo vadis* Internet?
- privacy and corporate responsibility;
- protecting the privacy of minors: a priority mission;
- privacy by design;
- towards a global regulation on privacy: proposals and strategies.

Data protection as a strategic element in the scope of business and international data transfers in a globalised world was one of the core issues at the conference. The conference was an opportunity to observe a growing demand from stakeholders, including civil society and industry, for a harmonised data protection framework across borders. It is in this spirit that the conference adopted a resolution welcoming draft international standards on the protection of personal data and privacy. These standards are the result of one year of intensive preparatory work coordinated by the Spanish authority, and they represent the first step towards a binding international instrument.

Surveillance systems are another issue that was thoroughly discussed in Madrid, especially those based on aspects of the human body, for instance biometrics, the use of which is spreading to various everyday areas.

Both the Supervisor and Assistant Supervisor participated in the conference. They respectively chaired the parallel session on 'Determining the applicable law in a world of globalisation', and intervened in the parallel session on 'Private life at work?'.

The next conference will take place in Jerusalem on 27–29 October 2010.

4.7. London initiative

At the 28th International Conference in London in November 2006, a statement was presented, entitled 'Communicating data protection and making it more effective', which received general support from data protection authorities around the world. This was a joint initiative of the president of the French data protection authority (CNIL), the UK Information Commissioner and the EDPS (since then referred to as the 'London initiative'). As one of the architects of the initiative, the EDPS is committed to contribute actively to the follow-up with national data protection authorities ([20]).

In the context of the London initiative, a number of workshops took place to exchange experience and share best practices in different areas, such as communication, enforcement, strategic planning and management of data protection authorities.

In April 2009, the EDPS organised a workshop for data protection authorities in Brussels for an exchange of best practices on 'Responding to security breaches'. This closed workshop also provided input to a seminar with other stakeholders on the subject, organised by the EDPS together with the European Agency for Network and Information Security (ENISA) and hosted by the European Parliament in October 2009.

4.8. International organisations

In November 2009, the EDPS and the European University Institute (EUI) began preparations for a third workshop on data protection in international organisations, to take place in spring 2010 in Florence.

Following the resolution on data protection and international organisations, adopted in 2003 at the International Conference in Sydney ([21]), the EDPS, together with the Council of Europe, the OECD and the European Patent Office, organised two previous workshops in Geneva (2005) and Munich (2007). International organisations which are exempted from national law often find themselves without a legal framework for data protection. These events highlighted their increasing interest in both protecting personal data and ensuring compliance within their organisations.

In this third workshop, the EDPS intends to focus the debate on the following issues:

- governance of data protection in international organisations;
- compliance in practice, notably in the management of human resources data;
- technological challenges and related security measures;
- use of biometrics at borders and for internal security purposes.

([20]) See Annual Report 2006, paragraphs 4.5 and 5.1.

([21]) http://www.privacyconference2008.org/adopted_resolutions/5-SYDNEY2003/SYDNEY-EN4.pdf

5

COMMUNICATION

5.1. Introduction

Information and communication play a key role in ensuring the visibility of the EDPS's main activities and in raising awareness both of the EDPS's work and of data protection in general. This is all the more important as the EDPS is still a young institution and, therefore, awareness of its role at EU level needs to be further consolidated. The first years following the establishment of the institution were primarily focused on this goal, which generally paid off in terms of increased visibility. Indicators such as the increased number of requests for information received from EU citizens, inquiries from the media, subscribers to the newsletter, as well as invitations to speak at conferences and traffic on the website all support the view that the EDPS has become a point of reference for data protection issues.

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 European 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.

Raising awareness and improving communication on relevant data protection issues was also an important objective of the 'London initiative' (see Section 4.7). One significant result of the first workshop in that context was the creation of a network of communication officers (with participation of the EDPS). Data protection authorities are using this network to exchange best practices and to carry out specific projects, such as the development of joint actions for relevant events.

Activities in 2009 were mainly dedicated to improving and developing the information and communication tools set up during the initial years of the institution, with a view to communicating more effectively and improving the reach to both the EU administration and the general public.

The Supervisor and Assistant Supervisor invested substantial time and effort in explaining their mission and raising awareness of data protection and a number of specific issues in different speeches throughout the year (see Annex G).

5.2. Communication 'features'

The EDPS's 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.

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's direct sphere of action is much more distinct. It is primarily focused on European 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's communication policy does not need to engage in a 'mass communication' strategy. Instead, awareness around data protection issues among EU citizens in the Member States essentially depends upon a more indirect approach, mainly via data protection authorities at national level, and the use of information centres and contact points.

The EDPS, however, does his part in raising his profile towards the general public, in particular through a number of communication tools (website, newsletter and other information materials), regularly liaising with interested parties (student visits to the EDPS's office for instance) and participating in public events, meetings and conferences.

Language policy

The EDPS's 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 so the language in which the EDPS communicates should be adapted accordingly. When it comes to information and communication tools aimed at a diverse audience, a clear and comprehensible language which avoids unnecessary jargon needs to be used. Constant efforts are therefore made in this direction with the aim of correcting the excessive 'legal' image of data protection.

When considering more specialised audiences (e.g. the media, data protection specialists, EU stakeholders), technical and legal terms are more appropriate. Therefore, the 'same news' may require being communicated using an adapted format and editing style, so as to correctly reflect the needs of the target audience.

5.3. Media relations

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

In 2009, the press service issued 14 **press releases**. Most of these related to new legislative opinions which were highly relevant to the public. Among

Peter Hustinx being interviewed by a journalist.

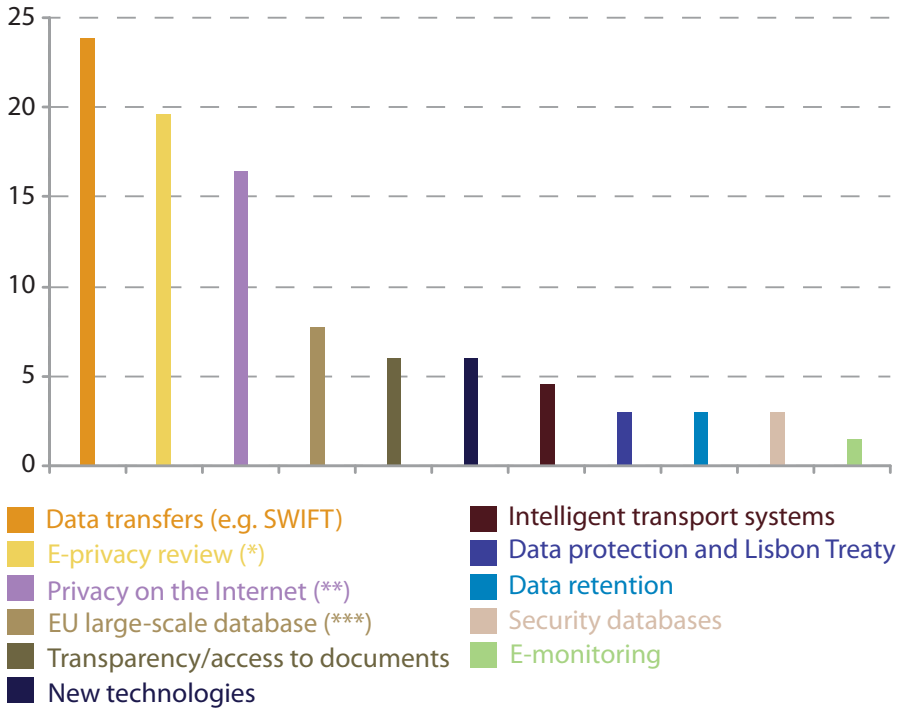
the issues covered were the review of the e-privacy directive, public access to EU documents, the new Stockholm programme in the area of justice and home affairs, intelligent transport systems in road transport, law enforcement access to Eurodac and the new agency for large-scale IT systems.

Press releases are published on the EDPS's website and on the European Commission's interinstitutional database of press releases (RAPID) in English and French. They 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, as they are often taken up 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 NGOs, academic institutions and information technology companies.

In 2009, the EDPS gave about 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 Belgian press. This resulted in a number of articles in the national, international and EU press, and publications and websites specialised in information technology issues, as well as interviews on radio and television (e.g. Franco-German television channel ARTE, Dutch radio, Swedish and Dutch television). The interviews covered horizontal issues such as European data security, the trend towards a surveillance society and the current and upcoming challenges in the field of privacy and data protection. They also addressed more focused matters, including the new EU–US SWIFT agreement, biometric passports and fingerprints databases, the new data breach notification requirement in the revised e-privacy directive, and the impact of the Lisbon Treaty on data protection.

Media enquiries are received on a regular basis and usually include requests for EDPS comments and requests for clarification or information. In 2009, media attention mainly focused on data transfer issues (e.g. the debate on a new SWIFT agreement), the review of the e-privacy directive (in particular the new provision on mandatory security breach notifications), privacy concerns on the Internet including search engines, new online applications and social networks, and large-scale EU databases. Access to EU documents and new technologies (such as RFID and cloud-computing) were also quite prominent issues for the press.

Main topics for requests from the press in 2009



(*) Including the new provision on data breach.

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

(***) Mainly Eurodac, CIS and VIS.

5.4. Requests for information and advice

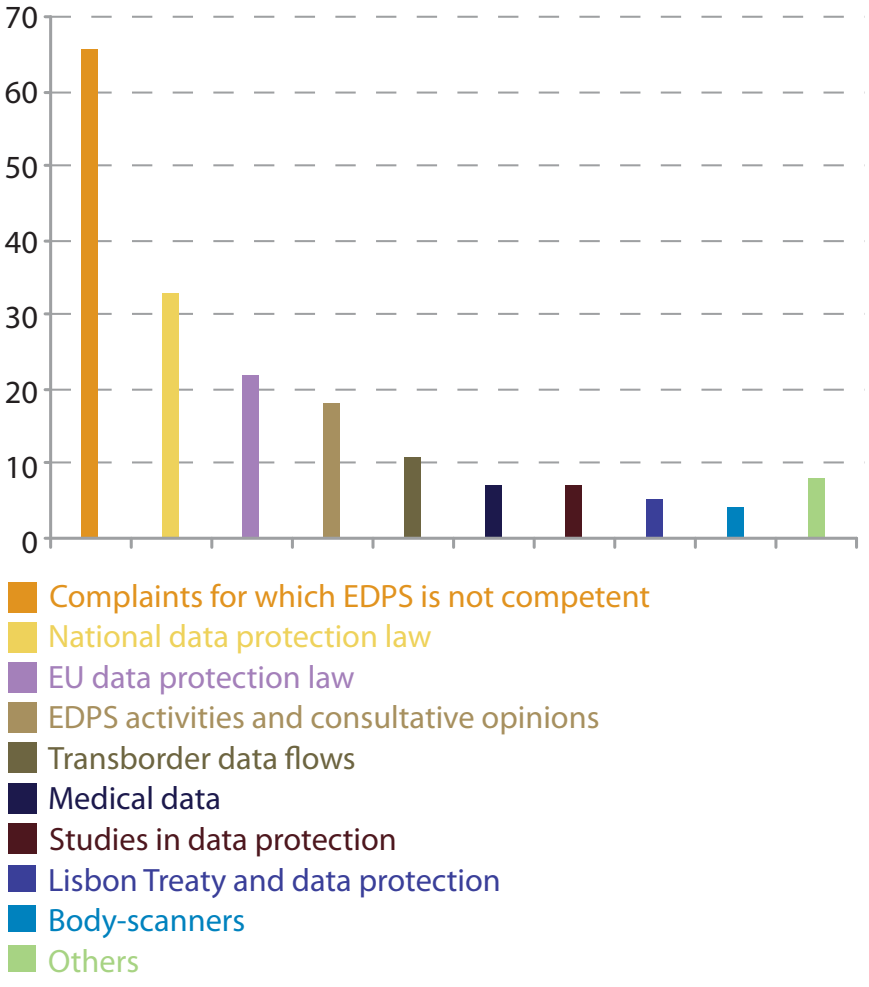
The number of enquiries for information or assistance received from citizens remained fairly stable in 2009 (174 requests compared with 180 in 2008). These requests come from a wide range of individuals and parties, ranging from stakeholders operating in the EU environment and/or working in the field of privacy, data protection and information technology (law firms, consultancies, lobbyists, NGOs, associations, universities, etc.) to citizens asking for more information on privacy matters or requiring assistance with relevant problems they have encountered. These requests are primarily received via the general e-mail account of the EDPS.

The first category of requests received in 2009 concerns complaints from EU citizens for which the EDPS has no competence. These complaints mostly related to alleged data protection breaches by national companies/public authorities, non-EU websites or online social networks. Others concerned an alleged privacy breach during a national court procedure and a request for appeal against a ruling from a national data protection authority. Given that these sorts of complaints fall outside the competence of the EDPS, a reply is sent specifying the mandate of the EDPS and advising that the complainant refer to the relevant authority, usually the national data protection authority of the appropriate Member State.

The second category of requests received in 2009 relates to data protection legislation in EU Member States and/or its implementation. In such cases, the EDPS advises the individual 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 EU data protection legislation, EDPS activities, transborder data flows, new data protection provisions in the Lisbon Treaty and data protection concerns related to the use of body scanners in airports.

Main areas of information requests from the public in 2009



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 specialised in the field of European law, data protection and/or IT security issues. For example, in October 2009, the EDPS office welcomed a group of international and European law students from the University of Grenoble in France to present its role and activities and discuss data protection matters in connection with the fight against terrorism. Other groups of visitors included Austrian MBA students in public management, and students from the University of Tilburg in the Netherlands.

With a view to reaching out to a younger audience, the EDPS office also welcomed a group of high-school students from Austria with whom staff members discussed data protection issues of particular interest to them, such as online social networks and the protection of minors on the Internet.

5.6. Online information tools

Website

The website continues to be the most important communication channel and information tool of the EDPS. 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's activities (e.g. opinions on prior checks and proposals for EU legislation, work priorities, publications, speeches and written contributions, press releases, newsletters, events information).

Content developments

In 2009, aside from an update to reflect the appointment of the Supervisor and the Assistant Supervisor for the second EDPS mandate, new information tools were published to further meet visitors' expectations and provide for a better understanding of the EDPS's activities. Such improvements included the publication of a glossary of terms related to the protection of personal data and a 'Questions and answers' section.

A thorough update of all the pages of the website was also carried out ahead of the introduction of a German version of the website in the course of 2010, in addition to the English and French versions. The development of a section on 'Frequently asked questions' is also in the pipeline in order to provide targeted answers to different profiles and audiences (e.g. EU staff, visitors, applicants to vacant posts in EU institutions and bodies).

Further improvements to the website are planned and will include the introduction of an online complaint form, the development of the Register of notifications and an overhaul of the homepage with a view to giving more prominence to the latest news on EDPS activities.

Technical developments and traffic

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 the website received a total of 92 884 unique visitors in 2009, including more than 8 000 per month in January, March, April, October and November. 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 e-mail or a link from another site — such as the Europa portal or a national data protection authority's website. Search engine 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.

Newsletter

The EDPS newsletter remains an effective tool to inform people about the latest EDPS activities, and to draw attention to recent additions to the website. The newsletter provides information on the latest EDPS opinions on EU legislative proposals and on prior checks. It also includes details about conferences and other events organised in the field, as well as recent speeches of the Supervisor and Assistant Supervisor. The newsletters are available on the EDPS's website and a subscription feature is offered on the relevant page.

Five issues of the EDPS newsletter were published in 2009, with an average frequency of one issue every two months. The newsletter is published in

English and French, with a German version to be expected in the course of 2010.

The number of subscribers rose from 880 at the end of 2008 to approximately 1 200 by the end of 2009. 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.

The substantial and steady increase in the number of subscriptions has led to the need to provide an upgraded and more user-friendly publication, together with a revised and more accessible structure. The first edition of the new version of the newsletter was published in October 2009.

5.7. Publications

Annual report

The Annual Report is the EDPS's key publication. It provides an overview of the EDPS activities in the main operational fields of supervision, consultation and cooperation during the reporting 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 the international, European and national levels — data subjects in general and EU staff in particular, the EU institutional system, data protection authorities, data protection specialists, interest groups and non-governmental organisations active in the field, journalists and anyone seeking information on the protection of personal data at EU level.

The Supervisor and Assistant Supervisor presented a summary of the EDPS Annual Report 2008 to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs on 16 April 2009.

Information brochure

In the context of the EDPS's second mandate (2009–14), a new information brochure was developed in 2009. Aimed at the public at large, the brochure provides information regarding the competences and duties of the EDPS, data subjects' rights, the role of data protection officers and the procedure for lodging a complaint to the EDPS. It also contains guidelines and short explanations on key elements of the role of the EDPS and the protection of personal data in the EU administration.

Thematic factsheets on specific data protection issues will be developed in 2010 in order to provide targeted information guidance to both the general public and interested parties.

5.8. Awareness-raising events

Participating in promotional events offers an excellent opportunity for the EDPS to raise awareness about the rights of the data subjects and the obligations of the European institutions and bodies in relation to privacy and data protection.

Data Protection Day

The member countries of the Council of Europe and the European institutions and bodies celebrated the third European Data Protection Day on 28 January 2009. 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 1981.

The EDPS used this opportunity to stress the importance of privacy and data protection, and in particular to raise awareness among EU staff about their rights and obligations in the field. An information stand was set up on three consecutive days in the European Parliament, the European Commission, and the Council premises. The EDPS outlined his supervisory, consultative and cooperative roles, as well as his achievements and current activities. The EDPS's stand was set up in cooperation with the data protection officers of the relevant institutions, who presented their activities as well. Various publications detailing the role of the EDPS and his work were distributed and visitors also had the opportunity to test their knowledge of data protection issues in a short quiz.

For the next edition of Data Protection Day the aim will be to further develop this activity, in particular through the use of video materials, and to diversify actions in this context so as to better reach EU staff members and other relevant parties.

EDPS stand at the European Commission during Data Protection Day.

EU Open Day

On 9 May 2009, the EDPS office participated, as it does now each year, in the Open Day at the European institutions organised in the European Parliament in Brussels.

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

6

ADMINISTRATION, BUDGET AND STAFF

6.1. Introduction

The first mandate of the two Supervisors ended in January 2009. After the elections which took place in 2008, a new team was appointed by the Council and the European Parliament for a five-year mandate.

In order to benefit from a reserve of highly specialised staff, the EDPS launched a general competition in data protection, organised by the European Personnel Selection Office (EPSO). The reserve list will be available in summer 2010.

The administrative environment is gradually being extended on the basis of annual priorities, taking into account the needs and size of the institution.

The EDPS has adopted new internal rules necessary for the proper functioning of the institution.

Collaboration with other institutions — the European Parliament, the Council and the European Commission — was further improved, allowing for considerable economies of scale.

6.2. Budget

The 2009 budget adopted by the budgetary authority amounted to EUR 6 663 026. This reflects an increase from 2008 due mainly to additional posts, the change of Supervisors and the increase in space required by the growth of the institution.

Apart from salaries and building expenses, a significant part of the budget is allocated to translations. The EDPS's opinions on legislative proposals are translated into 23 European official languages and are published in the *Official Journal of the European Union*. Opinions on prior checks and other published documents are also translated into the EDPS's working languages.

In its report on the 2008 financial year, the European Court of Auditors stated that the audit had not given rise to any observations.

Assistance from the European Commission continued, particularly in relation to accountancy services, since the Accounting Officer of the Commission is also appointed as the Accounting Officer of the EDPS. The EDPS applies the Commission's internal rules for the implementation of the budget. Those rules are applicable to the institution where specific rules have not been laid down.

6.3. Human resources

The EDPS benefits from the effective assistance of the European Commission's services with respect to the personnel management of the institution.

6.3.1. Recruitment

The growing visibility of the institution is leading to an increased workload and an expansion of tasks. The significant growth in workload in 2009 has been described in previous chapters and

human resources have an important role to play in this context. Nevertheless, the EDPS has chosen to limit the rate of expansion, using controlled growth to ensure that new staff are fully trained and integrated into the organisation.

The EDPS has access to the services provided by the European Personnel Selection Office (EPSO) and participates in the work of its management board, presently as an observer. In cooperation with EPSO, the EDPS has launched a general competition in data protection in order to recruit highly specialised staff. The reserve list will be available in summer 2010.

Concerning human resources management software (mainly for missions, holidays and training), the Commission suspended its former human resources management software project and created SYSPER2, which will be operational for the EDPS by the end of 2010.

6.3.2. Traineeship programme

A traineeship programme was created in 2005 with the aim of offering 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 EDPS with an opportunity to increase its visibility to younger EU citizens, particularly 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 addition to the main programme, special provisions were established to accept university and PhD students for the short term, as non-remunerated traineeships. This gives young students an opportunity to conduct research for their thesis. This is done in accordance with the 'Bologna process' and the obligation for these university students to complete a traineeship as part of their studies. These traineeships are limited to exceptional situations and under stringent admission criteria.

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 service level agreements signed in 2005 and 2008, 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 the data protection authorities (DPAs) of different Member States have been seconded every year. These secondments have enabled the EDPS to benefit from the skills and experience of such staff and served to increase the EDPS's visibility at national level. At the same time, this programme enables SNEs to familiarise themselves with data protection issues within the EU.

In order to recruit national experts, the EDPS contacts the national DPAs directly. National permanent representations are also informed of the programme and invited to assist in seeking suitable candidates.

6.3.4. Organisation chart

The EDPS's organisation chart has remained unchanged since 2004; namely: one unit, now consisting of eight people with responsibility for administration, staff and the budget; and the remaining members of staff, including a small team of coordinators in charge of the operational aspects, organised in two main fields: supervision and consultation. A press officer coordinates a small information team. They all work under the direct authority of the Supervisor, the Assistant Supervisor and a Director as Head of Secretariat.

At the end of 2009 the latter was introduced as a first step in a restructuring of the organisation to be expected in the course of 2010.

6.3.5. Training

The aim of the internal training policy to expand and improve staff knowledge and competencies, allowing a more effective contribution to the achievement of the institution's objectives, continued in 2009.

EDPS staff members have access to the training courses organised at interinstitutional level. Moreover, some staff members participated in professional external training with a view to achieving excellence in the field of data protection.

The training plan for 2009, including the staff needs identified through a survey, was based on the main learning areas identified in the general orientations, annexed to the internal training decision.

Language courses represented a significant part of the total number of days devoted to training in 2009. The high rate of participation confirms the principle that language learning in the EDPS should primarily serve to improve professional effectiveness and job-related needs including, of course, the harmonious integration of new staff into the organisation.

The EDPS continued to participate in interinstitutional committees — EAS's Inter-institutional Working Party, EAS's Inter-institutional Training Evaluation Group, Inter-institutional Committee for language training, etc. — with the aim of sharing a common approach in a sector where the needs are essentially similar across the institutions and allow for economies of scale.

In 2009, 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.

A service level agreement was also signed with the EAS allowing EDPS staff selected for the certification exercise to take part in the compulsory training programme for the certification procedure.

6.3.6. Social activities

New staff is personally welcomed by the Supervisor and the Assistant Supervisor. In addition to their mentor, they also meet with the members of the administrative unit who give them information on the specific procedures of the institution and the EDPS administrative guide. 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.

The EDPS is taking part as an observer in the European Parliament's advisory committee on prevention and protection at work, whose aim is to improve the work environment. A reflection has been launched on well-being at work.

The social dialogue within the EDPS had unfortunately to be stopped temporarily because of the resignation and non-renewal of the Staff Committee. A social activity outside the office could, however, be organised.

The EDPS continued to develop interinstitutional cooperation with regard to childcare: the children of EDPS staff have access to the crèches, the after-school childcare and the outdoor childcare centres of the Commission, as well as to the European Schools.

6.4. Control functions

6.4.1. Internal control

The internal control system, effective since 2006, ensures that EDPS objectives are achieved efficiently and in compliance with its 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.

In 2009, the assessment of risks related to the EDPS activities continued with the aim of designing a risk management system to identify, assess and where necessary take action to counteract any risks associated with its activities.

The EDPS took note of the annual activity report and the associated 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 the institution is responsible.

6.4.2. Internal audit

The Commission's internal auditor has been appointed internal auditor of the EDPS.

To ensure the effective management of EDPS resources, the internal auditor carries out regular checks of the institution's internal control systems as well as its financial operations.

A report relating to the follow-up audit carried out in December 2008 by the Internal Audit Service was received and adopted during 2009. The report confirmed the capacity of the EDPS's internal control system to provide reasonable assurance for the achievement of the institution's objectives, although it also identified some aspects that required improvement. Some of these have already been acted upon whilst others will be implemented gradually along with the evolution of the EDPS's tasks.

6.4.3. Security

At the end of 2008, the EDPS adopted a decision on the security measures applicable in the institution. The decision includes measures relating to the management of confidential information and IT security, as well as health and safety conditions for staff and premises. An information session was organised in 2009 to promote security awareness and ensure that staff were alert to the security measures in place.

6.4.4. Data protection officer

The internal implementation of the provisions of Regulation (EC) No 45/2001, concerning the protection of individuals with regard to the processing of personal data and the free movement of such data, continued in 2009.

Notifications to the data protection officer (DPO) of processing operations related to personal data identified in the EDPS inventory also continued in 2009. For cases subject to prior checking, notifications followed a simplified procedure which takes into account the specific position of the EDPS. A register of notifications has been set up.

Participation in DPO network meetings enables the EDPS's DPO to benefit from shared experiences and discuss common issues.

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 information technology (IT) and infrastructure.

The EDPS 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 interinstitutional cooperation

The EDPS benefits from interinstitutional cooperation in many areas of administration by virtue of the agreement concluded in 2004 and extended in 2006 (for a three-year period), with the Secretaries-General of the Commission, the Parliament and the Council. This cooperation is of considerable added value to the EDPS in terms of increased efficiency and economies of scale. It also avoids unnecessary multiplication of administrative infrastructure and reduction of unproductive administrative expenditure, whilst guaranteeing a high level of public service administration.

On this basis, interinstitutional cooperation continued in 2009 with various Commission Directorates-General (Personnel and Administration, Budget, Internal Audit Service, Education and Culture), the Paymaster's Office, various European Parliament services (IT services, particularly with arrangements for the new version of the EDPS's website; fitting out of the premises, building security, printing, mail, telephone, supplies, etc.) and with the Council (translations).

A service level agreement has been signed with the Paymaster's Office (PMO), covering a number of activities, including the determination, calculation and payment of individual rights of current and former staff, as well as the reimbursement of missions, healthcare and experts' expenses.

On the basis of positive evaluation, an extension of two years has been signed from January 2010 to January 2012. The agreement with the 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 will take over the translation work as from 2010.

Existing service level agreements are regularly updated. In November 2009, the EDPS signed a new service-level agreement with the European Administrative School relating to the staff training programme for the certification procedure.

Direct access from the EDPS's premises to some of the Commission's financial management applications facilitated cooperation and the exchange of information between Commission departments and the EDPS.

Ongoing cooperation with the European Parliament ensured the maintenance of the EDPS website and permitted the addition of new functionality.

The EDPS continued to participate in the interinstitutional calls for tenders, thus increasing its efficiency in many administrative areas and allowing progress towards greater autonomy.

The EDPS is a member of various interinstitutional committees and working groups, including the Comité de Gestion Assurances Maladies (CGAM), Comité de Préparation pour les Questions Statutaires (CPQS), Comité du Statut, the Inter-institutional Working Party/EAS, the Inter-institutional Training Evaluation Group and the Inter-institutional Committee for language training. This participation helped increase the visibility of the EDPS amongst the other institutions and encouraged the sharing of good practice.

6.6.2. Internal rules

The process of adopting new internal rules necessary for the proper functioning of the institution continued. New general implementing provisions for the Staff Regulations were also adopted.

Where these provisions relate to areas for which the EDPS benefits from the assistance of the Commission, they are similar to those of the Commission, albeit with some adjustments to allow for the specificities of the EDPS office.

On their first day, newcomers are provided with an 'Administrative guide', which contains all the EDPS's internal rules and specificities regarding the institution. This document is regularly updated.

A new guide to missions based on the one of the Commission has been adopted.

Three internal decisions were adopted in 2009, relating to the probationary period in cases of parental or family leave, special leave for breastfeeding mothers, and special leave for the serious illness of a child.

The EDPS is a relatively young institution and it has been developing fast. As a consequence, rules and procedures that are suitable during the first years of activity may prove less effective in the future, in the framework of a bigger and more complex structure. Existing rules will therefore be subject to an evaluation two years after their adoption and may be amended accordingly.

6.6.3. Document management

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

7

MAIN OBJECTIVES IN 2010

In the course of 2009, the first steps were taken for a strategic assessment of the roles and tasks of the EDPS in order to set out main lines of development for the next four years. This will have consequences in different areas, but particularly in the field of supervision and internal organisation. The developments in other areas will be more gradual along the lines described in this Annual Report.

The following main objectives have been selected for 2010. The results achieved on them will be reported next year.

- Support of DPO network

The EDPS will continue to give strong support to data protection officers, particularly in recently established agencies, and encourage an exchange of expertise and best practices, including the possible adoption of professional standards, in order to strengthen their effectiveness.

- Role of prior checking

The EDPS will put stronger emphasis on the implementation of recommendations in prior-checking opinions and ensure adequate follow up. Prior checking of processing operations common to most agencies will continue to receive special attention.

- Horizontal guidance

The EDPS will continue to develop guidance on relevant issues and make it generally available. Guidelines will be published on video-surveillance, administrative inquiries and disciplinary procedures, and implementing rules concerning the tasks and duties of data protection officers.

- Inspection policy

The EDPS will publish a comprehensive policy on the monitoring of compliance and enforcement of data protection rules in institutions and bodies. This will involve all appropriate means to measure and ensure compliance with data protection rules and encourage institutional responsibility for good data management.

- 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 to the action plan for the implementation of the Stockholm programme.

- Review of legal framework

The EDPS will give priority to the development of a comprehensive legal framework for data protection, covering all areas of EU policy and ensuring effective protection in practice, and contribute to the public debate where necessary and appropriate.

- Digital Agenda

The EDPS will give special attention to the Commission's Digital Agenda in all areas with an obvi-

ous impact on data protection. The principle of 'privacy by design' and its practical implementation will be strongly supported.

- Information activities

The EDPS will further improve its online information tools (website and electronic newsletter) to better meet visitors' demands. New publications ('factsheets') will be developed on thematic issues.

- Internal organisation

The EDPS will revise the organisational structure of its Secretariat in order to ensure a more effective and efficient execution of the different roles and tasks. The main lines of the new structure will be published on the website.

- Resource management

The EDPS will further develop activities relating to financial and human resources, and enhance other internal work processes. Special attention will be given to the need for additional office space and the development of a case management system.

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 the 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 of the EC Treaty, the European Data Protection Supervisor was established by Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, which entered into force in 2001 ([22]). 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 abovementioned article 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 countries 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 of the EC Treaty, 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 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'. Since the entry into force of the Lisbon Treaty, this means that EU institutions and bodies that used to be 'Community institutions and bodies' are subject to the supervisory tasks and powers of the EDPS. It is unclear whether the regulation has a wider scope and extends into parts of the former 'third pillar'.

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

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

ARES	Advanced records system
CCL	Common Conservation List
CCTV	Closed circuit television
CdT	Translation Centre for the Bodies of the European Union
Cedefop	European Centre for the Development of Vocational Training
CFCA	Community Fisheries Control Agency
CIS	Custom information system
CJ	Court of Justice of the European Union
CoR	Committee of the Regions
CPCS	Consumer protection cooperation system
CPVO	Community Plant Variety Office
CRS	Computerised reservation system
DPA	Data protection authority
DPC	Data protection coordinator (only in the European Commission)
DPO	Data protection officer
EAS	European Administrative School
EC	European Communities
ECA	European Court of Auditors
ECB	European Central Bank
ECRIS	European criminal records information system
EESC	European Economic and Social Committee
EFSA	European Food Safety Authority
EIB	European Investment Bank
EMPL	Committee on Employment and Social Affairs in European Parliament
ENISA	European Network and Information Security Agency
ECHR	European Convention on Human Rights
EMA	European Medicines Agency
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMSA	European Maritime Safety Agency
EPSO	European Personnel Selection Office
ETF	European Training Foundation
EU	European Union
EUMC	European Monitoring Centre on Racism and Xenophobia
Eurofound	European Foundation for the Improvement of Living and Working Conditions
EWS	Early warning system
FIDE	Customs Files Identification Database
FP7	Seventh research framework programme
FRA	European Union Agency for Fundamental Rights
IAS	Internal Auditing Service
IGC	Inter-Governmental Conference
IMI	Internal market information system
IMS	Identity Management Service
JRC	Joint Research Centre
JSB	Joint supervisory body
LIBE	Committee on Civil Liberties, Justice and Home Affairs in European Parliament
MoU	Memorandum of understanding

NSA	National security authority
OECD	Organisation for Economic Cooperation and Development
OHC	Occupation Health Centre
OHIM	Office for Harmonization in the Internal Market
OLAF	European Anti-Fraud Office
PEP	Politically exposed person
PMO	European Commission Paymaster's Office
PNR	Passenger name record
R & D	Research and development
RFID	Radio frequency identification
SIS	Schengen information system
SOC	Service and operational centre
s-TESTA	Secure trans-European services for telematics between administrations
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFUE	Treaty on the Functioning of the European Union
TIM	Time management system
VIS	Visa information system
WP29	Article 29 Working Party
WPPJ	Working Party on Police and Justice

Annex D — List of data protection officers

ORGANISATION	NAME	E-MAIL
European Parliament	Jonathan STEELE	Data-Protection@europarl.europa.eu
Council of the European Union	Pierre VERNHES	Data.Protection@consilium.europa.eu
European Commission	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Court of Justice of the European Union	Marc SCHAUSS	Dataprotectionofficer@curia.europa.eu
European Court of Auditors (ECA)	Jan KILB	Data-Protection@eca.europa.eu
European Economic and Social Committee (EESC)	Maria ARSENE	Data.Protection@eesc.europa.eu
Committee of the Regions (CoR)	Petra CANDELLIER	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)	Giuseppina LAURITANO	Giuseppina.Lauritano@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 (EMA)	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
European Food Safety Authority (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu

>>>

ORGANISATION	NAME	E-MAIL
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 (EU-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	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)	Elisa DALLE MOLLE	Elisa.Dalle-Molle@ec.europa.eu
European Chemicals Agency (ECHA)	Minna HEIKKILA	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
Fusion for Energy Joint Undertaking (European Joint Undertaking for ITER and the Development of Fusion Energy)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu

>>>

ORGANISATION	NAME	E-MAIL
SESAR Joint Undertaking	Daniella PAVKOVIC	Daniella.PAVKOVIC@sesarju.eu
ARTEMIS Joint Undertaking	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Clean Sky Joint Undertaking	Silvia POLIDORI	Silvia.Polidori@cleansky.eu
Innovative Medecines Initiative (IMI) Joint Undertaking	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Fuel Cells and Hydrogen Joint Undertaking	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu

Annex E — List of prior-check opinions

Evaluation procedures — EMA

Opinion of 18 December 2009 on the performance evaluation procedures of the European Medicines Agency (Case 2007-421)

Postes individuels — Parlement

Avis du 17 décembre 2009 sur la notification d'un contrôle préalable à propos du dossier 'Postes individuels' (Dossier 2009-650)

Procédure de notation — Conseil

Avis du 15 décembre 2009 sur la notification d'un contrôle préalable à propos du dossier 'Procédure de notation des fonctionnaires du Conseil' (Dossier 2009-042)

Selection of a Director for EIGE — Parliament

Opinion of 8 December 2009 on a notification for prior checking on the selection of a Director for the European Institute for Gender Equality (EIGE) (Case 2008-785)

EudraVigilance data quality management system — EMA

Opinion reflected in a letter of 7 December 2009 on the notification for prior checking of the EudraVigilance data quality management system (Case 2009-740)

Leave management — EFSA

Opinion of 1 December 2009 on a notification for prior checking concerning 'EFSA leave management' (Case 2009-455)

Mobilité interne — Banque européenne d'investissement

Avis du 18 novembre 2009 sur la notification de contrôle préalable à propos du dossier 'mobilité interne' (Dossier 2009-253)

Vérification des pointages Flexitime — Conseil

Avis du 12 novembre 2009 sur la notification de contrôle préalable à propos du dossier 'Vérification des pointages Flexitime par rapport aux données sur l'accès physique' (Dossier 2009-477)

Enquêtes administratives et procédures disciplinaires — CESE

Avis du 9 novembre 2009 sur la notification de contrôle préalable à propos du dossier 'Enquêtes administratives et procédures disciplinaires internes au CESE' (Dossier 2008-569)

EAS Emotional Intelligence 360 degree assessment — Commission

Opinion of 30 October 2009 on a notification for prior checking concerning 'EAS (European Administrative School) — Emotional Intelligence 360 degree assessment' (Case 2009-100)

Assurances des députés — Parlement

Avis du 27 octobre 2009 sur la notification de contrôle préalable à propos du dossier 'Assurances des députés' (Dossier 2009-434)

'e-performance' — Banque européenne d'investissement

Avis du 19 octobre 2009 sur la notification d'un contrôle préalable à propos du dossier 'e-performance' (Dossier 2008-379)

Exploitation des listes de réserve — Cour des comptes

Avis du 5 octobre 2009 sur la notification d'un contrôle préalable à propos du dossier 'exploitation des listes de réserve et des listes d'aptitude pour le recrutement de fonctionnaires, agents temporaires et contractuels' (Dossier 2008-433)

Gestion du Centre Polyvalent de l'Enfance (CPE) — Commission

Avis du 29 septembre 2009 sur la notification d'un contrôle préalable à propos du dossier 'Gestion du Centre Polyvalent de l'Enfance (CPE) — Garderie et Centre d'études: système d'information Loustic et dossiers médicaux' (Luxembourg) (Dossier 2009-089)

Security support system — Parliament

Opinion of 29 September 2009 on a notification for prior checking concerning the 'Security support system' (Case 2009-225)

Selection of permanent and temporary staff — Council

Opinion of 28 September 2009 on the notification for prior checking on the 'selection of permanent and temporary staff at the General Secretariat of the Council of the European Union' (Case 2009-197)

Selection and recruitment of temporary and contractual agents — FRA

Opinion of 24 September 2009 on the notification for prior checking regarding FRA's selection and recruitment of its temporary and contractual agents (Case 2008-589)

Disciplinary Board — Commission

Opinion of 21 September 2009 on the notification for prior checking on the 'Disciplinary Board' case (Case 2009-087)

Accident insurance — Council

Opinion of 14 September 2009 on the notification for prior checking concerning 'Data processing with regard to accident insurance' (Case 2009-257)

EudraVigilance database — EMA

Opinion of 7 September 2009 on a notification for prior checking regarding the EudraVigilance database (Case 2008-402)

Evaluation of the President and the Vice-President — CPVO

Opinion of 28 July 2009 on a notification for prior checking concerning 'Evaluation of the President and the Vice-President of the CPVO' (Cases 2009-355 and 2009-356)

Temps partiel — Comité des régions

Avis du 27 juillet 2009 sur la notification d'un contrôle préalable à propos des demandes d'exercice de l'activité à temps partiel (Dossier 2009-396)

Temps partiel — Comité économique et social

Avis du 24 juillet 2009 sur la notification d'un contrôle préalable à propos des demandes d'exercice de l'activité à temps partiel (Dossier 2009-322)

Recrutement — Cour des comptes

Avis du 23 juillet 2009 sur la notification d'un contrôle préalable à propos du dossier 'procédures de sélection pour le recrutement de fonctionnaires, agents temporaires et agents contractuels' (Dossier 2008-313)

Hearings of the Commissioners-designate — Parliament

Opinion of 3 July 2009 on a notification for prior checking on the processing of personal data in the hearings of the Commissioners-designate (Case 2009-0332)

Training evaluation — European Central Bank

Opinion of 1 July 2009 on a notification for prior checking regarding training evaluation (Case 2009-220)

Call for tender procedures — EESC

Opinion of 30 June 2009 on the call for tender procedures and management of contracts (Case 2009-323)

Time and absence management — ECDC

Opinion of 22 June 2009 on the notification for prior checking concerning 'Time and absence management' (Case 2009-072)

Selection of middle management and advisers — Commission

Opinion of 17 June 2009 on a notification for prior checking regarding the selection of middle management staff and advisers in the Commission (Case 2008-751)

Recruitment of contract staff — Committee of the Regions

Opinion of 16 June 2009 on the notification for prior checking regarding the 'recruitment of contract staff' (Case 2008-696)

Recruitment of officials — Committee of the Regions

Opinion of 16 June 2009 on the notification for prior checking regarding the 'recruitment of officials' (Case 2008-694)

Recruitment of temporary staff — Committee of the Regions

Opinion of 16 June 2009 on the notification for prior checking regarding the 'recruitment of temporary staff' (Case 2008-695)

Documents provided during recruitment — Commission

Opinion of 5 June 2009 on a notification for prior checking on documents provided during recruitment (Case 2008-755)

Specific declarations of interest — EFSA

Opinion of 5 June 2009 on a notification for prior checking regarding the 'Handling of annual and specific declarations of interest' (Case 2008-737)

Administering traineeships — Commission

Opinion of 5 June 2009 on the notification for prior checking regarding the 'Application for administering traineeships' (Case 2008-485)

Safety at work at JRC — Commission

Opinion of 20 May 2009 on the notification for prior checking regarding the management of safety at work at the Joint Research Centre's Institute for Health and Consumer Protection in Ispra (Case 2008-541)

Enterprise Data Warehouse — Commission

Opinion of 19 May 2009 on the notification for prior checking regarding the processing of personal data in DG ENTR Enterprise Data Warehouse (Case 2008-487)

Prevention of harassment — Parliament

Opinion of 19 May 2009 on the notification for prior checking regarding the prevention of harassment (Case 2008-477)

Trainee applications and recruitment — EMA

Opinion of 18 May 2009 on a notification for prior checking regarding trainee applications and recruitment (Case 2008-730)

Promotion and regarding procedure — CdT

Opinion of 18 May 2009 on the notification for prior checking concerning the promotion and regarding procedure case (Case 2009-018)

Mediation Service — Commission

Opinion of 18 May 2009 on the notification for prior checking on the 'Mediation Service of the European Commission' (Case 2009-010)

TFlow and PROFIL — Parliament

Opinion of 8 May 2009 on a notification for prior checking regarding the processing operation 'TFlow' and 'PROFIL' (Case 2009-069)

Staff recruitment procedures in certain Community agencies

Opinion of 7 May 2009 on notifications for prior checking of certain Community agencies concerning the 'Staff recruitment procedures' (Case 2009-287)

Assessment and reporting on probationary periods — EFSA

Avis du 6 mai 2009 sur la notification de contrôle préalable concernant les 'Evaluations et rapports de stage' (Dossier 2009-030)

Horaire flexible — Cour de justice

Avis du 6 mai 2009 sur la notification d'un contrôle préalable de la Cour de justice à propos du dossier 'horaire flexible' (Dossier 2007-437)

Annual dialogue — ETF

Opinion of 4 May 2009 on a notification for prior checking concerning 'ETF annual dialogue' (Case 2009-168)

Voice logging at JRC-IE — Commission

Opinion of 29 April 2009 on a notification for prior checking on voice logging at the Joint Research Centre Institute for Energy (JRC-IE) in Petten (Case 2008-014)

Medical data of children attending interinstitutional crèches — Commission

Opinion of 27 April 2009 on a notification for prior checking on the management of the medical data of children attending the interinstitutional crèches and kindergartens managed by the OIB (Case 2009-088)

Selection procedures for seconding national experts — FRA

Avis du 27 avril 2009 sur la notification de contrôle préalable concernant les procédures de sélection des experts nationaux détachés (Dossier 2008-747)

Junior experts in delegation — Commission

Opinion of 22 April 2009 on the notification for prior checking regarding 'Junior Experts in Delegation' (Case 2008-754)

Early retirement — European Economic and Social Committee

Opinion of 1 April 2009 on the notification for prior checking on the annual exercise for early retirement without reduction of pension rights (Case 2008-719)

Structural trainees — Commission

Opinion of 30 March 2009 on the notification for prior checking regarding structural trainees (Case 2008-760)

Waiver of immunity from legal proceedings and inviolability of Commission premises and archives — Commission

Opinion of 25 March 2009 on the notification for prior checking concerning 'the processing of requests for waiver of immunity from legal proceedings and of the inviolability of Commission premises and archives' (Case 2008-645)

Management of information sent by OLAF — Commission

Opinion of 23 March 2009 on a notification for prior checking on the management of information sent by OLAF under memorandum of understanding (Case 2009-011)

End-of-probation procedure — Commission

Opinion of 10 March 2009 on the notification for prior checking concerning the 'end-of-probation procedure' case (Case 2008-720)

Flexitime — ETF

Opinion of 26 February 2009 on a notification for prior checking regarding ETF — Flexitime procedure (Case 2008-697)

Staff Guidance and Reinstatement Group — Council

Opinion of 23 February 2009 on the notification for prior checking on the Staff Guidance and Reinstatement Group (Case 2008-746)

Temporary agents — Community Plant Variety Office

Opinion of 20 February 2009 on a notification for prior checking regarding the engagement and use of temporary agents (Case 2008-315)

Early retirement — Parliament

Opinion of 18 February 2009 on a notification for prior checking on the procedure for early retirement without reduction of pension rights (Case 2008-748)

ART: Audit Reconciliation Tool — Court of Auditors

Opinion of 9 February 2009 on a notification for prior checking regarding 'ART: Audit Reconciliation Tool' (Case 2008-239)

Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme — Commission

Avis du 26 janvier 2009 sur la notification de contrôlé préalable à propos du dossier 'Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme' (Dossier 2008-440)

Capacity to work in a third language before first promotion — Parliament

Opinion of 21 January 2009 on a notification for prior checking on the assessment of staff's capac-

ity to work in a third language before first promotion (Case 2008-690)

Report on probation period — Parliament

Opinion of 21 January 2009 on a notification for prior checking concerning the report on probation period (Case 2008-604)

Invalidity Committee — Council

Opinion of 16 January 2009 on the notification for prior checking regarding the 'Invalidity Committee procedure' (Case 2008-626)

Training SYSLOG — Commission

Opinion of 16 January 2009 on a notification for prior checking on the management of Central and Local Training SYSLOG Formation (Case 2008-481)

Management of the crèche — Council

Opinion of 15 January 2009 on the notification for prior checking on the 'Management of the crèche of the General Secretariat of the Council and billing' case (Case 2007-441)

Early retirement — Court of Auditors

Opinion of 9 January 2009 on the notification for prior checking on the 'Annual exercise for early retirement without reduction of pension rights' (Case 2008-552)

Annex F — List of opinions on legislative proposals

Restrictive measures in respect of Somalia e.a.

Opinion of 16 December 2009 on various legislative proposals imposing certain specific restrictive measures in respect of Somalia, Zimbabwe, the Democratic Republic of Korea and Guinea

Agency for large-scale IT systems

Opinion of 7 December 2009 on the proposal for a regulation establishing an agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council decision conferring upon the agency tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty

Combating fraud in the field of value added tax

Opinion of 30 October 2009 on the proposal for a Council regulation on administrative cooperation and combating fraud in the field of value added tax (recast)

Law enforcement access to Eurodac

Opinion of 7 October 2009 on the proposals regarding law enforcement access to Eurodac

Restrictive measures in respect of Al Qaida and the Taliban

Opinion of 28 July 2009 on the proposal for a Council regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban (OJ C 276, 17.11.2009, p. 1)

Intelligent transport systems

Opinion of 22 July 2009 on the communication from the Commission on an action plan for the deployment of intelligent transport systems in Europe and the accompanying proposal for a directive of the European Parliament and of the Council laying down the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other transport modes

'Stockholm programme' — An area of freedom, security and justice serving the citizen

Opinion of 10 July 2009 on the communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen (OJ C 276, 17.9.2009, p. 8)

Pharmaco-vigilance

Opinion of 22 April 2009 on the proposals for a regulation and for a directive on pharmaco-vigilance (OJ C 229, 23.9.2009, p. 19)

Use of information technology for customs purposes

Opinion of 20 April 2009 on the initiative of the French Republic for a Council decision on the use of information technology for customs purposes (OJ C 229, 23.9.2009, p. 12)

Collection of statistical information by the European Central Bank

Opinion of 8 April 2009 on the Recommendation for a Council regulation amending Regulation (EC) No 2533/98 concerning the collection of statistical information by the European Central Bank (OJ C 192, 15.8.2009, p. 1)

Organ transplantation

Opinion of 5 March 2009 on the proposal for a directive on standards of quality and safety of human organs intended for transplantation (OJ C 192, 15.8.2009, p. 6)

Common fisheries policy

Opinion of 4 March 2009 on the proposal for a Council regulation establishing a Community control system for ensuring compliance with the rules of the common fisheries policy (OJ C 151, 3.7.2009, p. 11)

Asylum: Eurodac regulation

Opinion of 18 February 2009 on the proposal for a regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...]

[establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (COM(2008) 825; OJ C 229, 23.9.2009, p. 6)

Asylum: Dublin regulation

Opinion of 18 February 2009 on the proposal for a regulation establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (COM(2008) 820 final); OJ 229, 23.9.2009, p. 1)

Minimum stocks of crude oil and petroleum products

Opinion of 3 February 2009 on the proposal for a Council directive imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ C 128, 6.6.2009, p. 42)

Second opinion on e-privacy

Second opinion of 9 January 2009 on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications) (OJ C 128, 6.6.2009, p. 28)

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.

The Supervisor frequently appeared in the European Parliament's LIBE Committee or at related events. On 5 March, he spoke at a hearing on challenges for fundamental rights on the Internet. On 16 April, he presented together with the Assistant Supervisor the main lines of the Annual Report 2008 of the EDPS. On 27 April, he spoke about the ongoing revision of Regulation (EC) No 1049/2001 on public access to documents. On 22 July, he presented the EDPS opinion on the Commission's communication on the Stockholm programme. On 3 September, he spoke at the Joint Meeting of LIBE and ECON Committees on the EU–US interim agreement about SWIFT. On 29 September, the Assistant Supervisor spoke in the LIBE Committee on the use of information technology for customs purposes. On 30 March, he spoke in the European Parliament's ENVI Committee on data protection issues as regard the proposal for a directive on organ transplantation.

The Supervisor also appeared in other meetings with the European Parliament. On 22 January, he spoke in the TRAN Committee at a hearing on intelligent transport systems. On 28 January, he contributed to the celebration of Data Protection Day in the Parliament. On 10 February, he presented the EDPS opinion on patients' rights in cross-border healthcare in the ENVI Committee. On 29 September, he spoke at a meeting of the European Privacy Association in cooperation with different Members of the European Parliament.

On 26 January, the Supervisor contributed to the celebration of Data Protection Day in the Polish Permanent Representation in Brussels. On 5 March, he spoke in the Council on the revision of Regulation (EC) No 1049/2001 on public access to documents. On 23 March, he spoke in the Council's Working Party on Data Protection about priorities in supervision and consultation. On 6 July, he delivered a speech on the need for an EU information management strategy at the first meeting under the Swedish Presidency of the Council Working Party on Information Exchange. On 15 July, the Assistant Supervisor spoke at the Council Working Group on e-Justice and interconnection of insolvency registers. On 7 December, the Supervisor was at a House of Commons' Committee hearing on data protection and law enforcement at the UK Permanent Representation in Brussels. On 28 October the Assistant Supervisor delivered a speech at the Berlin State Parliament in a celebration of 30 years of data protection and of 10 years of freedom of information in Germany.

On 26 March, the Assistant Supervisor spoke at a European Economic and Social Committee hearing on the deployment of intelligent transport systems in Ostrava. On 28 April, the Supervisor presented on strategic issues in data protection at a meeting of RISEPTIS, the Commission's Advisory Board for Research and Innovation on Security, Privacy and Trustworthiness in the Information Society. On 12 May, he spoke at a meeting of the SIS-VIS Committee on data security issues. On 14 May, he delivered a speech at the Commission's conference on the evaluation of the directive on data retention. On 20 May, the Supervisor and the Assistant Supervisor both spoke at the Commission's Data Protection Conference. On 14 September, the Assistant Supervisor spoke at a European Economic and Social Committee hearing on social networks in Brussels. On 16 September, the Supervisor spoke at a conference organised by the European Network and Information Security Agency (ENISA) in Heraklion. On 30 September, the Assistant Supervisor spoke at the EDPS workshop on video-surveillance within Community institutions and bodies. On 13 May he spoke on data protection within EU institutions and bodies at the 12th Agency Legal Network (IALN) meeting, held by the Office for Harmonization in the Internal market (OHIM) in Alicante. On 4 April he spoke at an International Conference on Freedom of Information and Data Protection in Viareggio. On 23 October, the Supervisor and the Assistant Supervisor both contributed to a seminar on data breach organised by the EDPS in cooperation with ENISA.

On 16 January, the Supervisor spoke on data protection in the context of Schengen and Dublin at the University of Fribourg, Switzerland. On 17 January, he spoke at the annual conference on 'Computers, privacy and data protection' in Brussels. On 27 January, he contributed to a conference on data protection and law enforcement at the Clingendael Institute in The Hague. On 11 February,

he spoke on current challenges for European data protection at a TEPSA conference in Brussels. On 19 February, he presented at the E-Health 2009 conference in Prague. On 27 February, he addressed an advisory board on e-government issues in The Hague. On 19 March, he contributed to a PES conference on the Internet in Athens. On 26 March, he spoke at a conference of the British Bankers' Association in London. On 3 November the Assistant Supervisor spoke on recent developments on data protection at European level at a FIDE workshop (Spanish Foundation on Investigation on Law and Enterprise) in Madrid. On 14 December he delivered a keynote speech at the University of Florence on data protection and codes of conduct, and on 17 April he spoke at the Alma Graduate School in Bologna on e-monitoring in the workplace.

On 28 April, the Assistant Supervisor delivered a speech on privacy and security at the Centre for European Policy Studies in Brussels. On 8 May, the Supervisor contributed to a conference on the 'Internet of things' in Brussels. On 18 May, he spoke at a conference on EU data protection in Brussels. On 21 May, he delivered a speech at the Spring Conference of the Austrian Commission of Jurists in Weissenbach am Attersee. On 8 June, he spoke at the 11th Conference on Data Protection and Data Security in Berlin. On 19 June, the Assistant Supervisor intervened at a conference of European judiciaries on surveillance and protection of fundamental rights in Vienna. On 23 June (privacy and security at global level) and 10 September (European Court cases on data protection), he spoke at two Italian Superior Council for the Judiciary conferences (CSM) for judges and public prosecutors.

On 8 September, the Supervisor delivered a speech at the Seminar 'Transparency and clear legal language in the EU', organised by the Swedish Presidency in Stockholm. On 21 September, he spoke at a conference on government and IT in Antwerp. On 24 September, he visited the Slovak data protection authority in Bratislava. On 8 October, he spoke at the 35th anniversary of the Dutch section of the International Commission of Jurists (NJCM) in The Hague. On 8–9 October, the Supervisor and the Assistant Supervisor contributed to a workshop on data protection in criminal proceedings in Strasbourg. On 13 October, the Supervisor spoke at a meeting of the OECD Working Party on Information Security and Privacy in Paris. On 14 October, he contributed to a conference on security and privacy in Oslo. On 26 October, he spoke at a lunch meeting of the Belgian-Dutch Association (BENEV) in Brussels. On 28 October, he spoke at a conference of Missing Children Europe in Brussels.

On 2 November, the Supervisor spoke at a workshop on privacy by design in Madrid. On 3 November, he addressed a civil society conference in Madrid. On 12 November, he spoke at a seminar on the Stockholm programme, organised by the Robert Schuman Foundation in Brussels, and at a BEUC conference on consumer privacy in Brussels. On 20 November, he delivered a speech at a Dutch national privacy conference in Amsterdam. On 2 December, he spoke on e-health issues at a conference organised by the Friends of Europe in Brussels. On 3 December, he spoke on intelligent transport systems at the Ninth Freight Forwarders Conference in Brussels.

The Supervisor and the Assistant Supervisor were also involved in transatlantic relations. On 12 March, the Supervisor presented at the IAPP Privacy Summit in Washington DC. On 26 May, the Assistant Supervisor delivered a speech at the first Euro-Ibero American Seminar on Data Protection in Cartagena de Indias, Colombia. On 16–18 November, the Supervisor and Assistant Supervisor contributed to the Safe Harbor Conference organised by the US Department of Commerce in Washington DC.

Annex H — Composition of EDPS Secretariat

Monique LEENS-FERRANDO
Head of Secretariat (since November 2009)

• Supervision

Sophie LOUVEAUX *Administrator/Legal Officer* *Coordinator DPO Relations and Prior Checks*	Manuel GARCIA SANCHEZ *National Expert/Technology Officer* *(until October 2009)*
Zsuzsanna BELENYESSY *Administrator/Legal Officer*	John-Pierre LAMB *National Expert (since October 2009)*
Isabelle CHATELIER *Administrator/Legal Officer*	Xanthi KAPSOSIDERI *Supervision Assistant*
Eva DIMOVNÉ KERESZTES *Administrator/Legal Officer* *Coordinator Inspections* *(until October 2009)*	Sylvie PICARD *Supervision Assistant*
Jaroslaw LOTARSKI *Administrator/Legal Officer* *Coordinator Complaints*	Kim Thien LÊ *Secretariat Assistant*
Maria Veronica PEREZ ASINARI *Administrator/Legal Officer* *Coordinator Administrative Measures*	Pierre FALLER *Trainee (April 2009 to July 2009)*
Tereza STRUNCOVA *Administrator/Legal Officer*	Evangelia MESAIKOU *Trainee (March 2009 to July 2009)*
Michaël VANFLETEREN *Administrator/Legal Officer*	Eleni ATHERINOU *Trainee (since October 2009)*
Athena BOURKA *National Expert/Technology Officer* *(until October 2009)*	Mathias POCS *Trainee (since October 2009)*

• Policy and information

Hielke HIJMANS *Administrator/Legal Officer* *Coordinator Consultation and Court Procedures*	Roberto LATTANZI *National Expert (since October 2009)*
Rosa BARCELO *Administrator/Legal Officer*	Martine BLONDEAU (*) *Documentation Assistant*
Laurent BESLAY *Administrator/Technology Officer* *Coordinator Security and Technology*	Francisco Javier MOLEÓN GARCIA *Documentation Assistant*
Katarzyna CUADRAT-GRZYBOWSKA *Administrator/Legal Officer*	Andrea BEACH *Secretariat Assistant*
Bénédicte HAVELANGE *Administrator/Legal Officer* *Coordinator Large IT Systems and Border Policy*	Anna-Maria VANHOYE *Secretariat Assistant* *(since October 2009)*
Herke KRANENBORG *Administrator/Legal Officer*	Vasiliki MYLONA *Trainee (March 2009 to July 2009)*
Anne-Christine LACOSTE *Administrator/Legal Officer* *Coordinator Article 29 Working Party*	Mario VIOLA DE AZEVEDO CUNHA *Trainee (March 2009 to July 2009)*
Alfonso SCIROCCO *Administrator/Legal Officer*	Maria-Grazia PORCEDDA *Trainee (since October 2009)*
Nathalie VANDELLE (*) *Administrator/Press Officer* *Coordinator Information Team*	

(*) Information Team.

• Personnel/Budget/Administration Unit

Monique LEENS-FERRANDO
Head of Unit (until October 2009)

• Human resources

Giuseppina LAURITANO *Administrator/Statutory Questions* *Audit and Data Protection Officer*	Guido CAGNONI *Trainee (March 2009 to July 2009)*
Vittorio MASTROJENI *Human Resources Assistant*	Livia HARSEU *Trainee (since October 2009)*
Anne LEVÊCQUE *Human Resources Assistant*	

• Budget and finance

Tonny MATHIEU *Finance Administrator (until October 2009)*	Maria SANCHEZ LOPEZ *Finance and Accounting Assistant*
Raja ROY *Finance and Accounting Assistant*	

• Administration

Anne-Françoise REYNDERS *Social activities, Infrastructure, Administration Assistant*

The EDPS and Assistant EDPS with their staff.

The European Data Protection Supervisor

Annual Report 2009

Luxembourg: Publications Office of the European Union

2010 — 108 pp. — 21 x 29.7 cm

ISBN 978-92-95073-07-4
doi:10.2804/10631

EUROPEAN DATA
PROTECTION SUPERVISOR

QT-AA-10-001-EN-C

The European guardian of personal data protection

www.edps.europa.eu

Publications Office

ISBN 978-92-95073-07-4