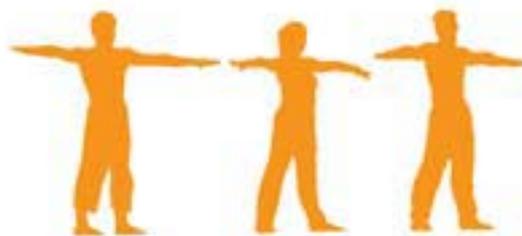


# Annual Report

**2006**



EUROPEAN DATA  
PROTECTION SUPERVISOR





# Annual Report

## 2006



EUROPEAN DATA  
PROTECTION SUPERVISOR

Postal address: EDPS, rue Wiertz 60, B-1047 Bruxelles  
Office address: rue Montoyer 63, Bruxelles  
E-mail: [edps@edps.europa.eu](mailto:edps@edps.europa.eu)  
Internet: [www.edps.europa.eu](http://www.edps.europa.eu)  
Tel. (32-2) 283 19 00  
Fax (32-2) 283 19 50

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: Office for Official Publications of the European Communities, 2007

ISBN 92-95030-12-5

© European Communities, 2007

Reproduction is authorised provided the source is acknowledged.

*Printed in Belgium*

PRINTED ON WHITE CHLORINE-FREE PAPER

# Table of contents

User guide	7
Mission statement	9
Foreword	11
<b>1. Balance and perspectives</b>	<b>13</b>
<b>1.1. General overview of 2006</b>	<b>13</b>
<b>1.2. Results in 2006</b>	<b>13</b>
<b>1.3. Objectives for 2007</b>	<b>14</b>
<b>2. Supervision</b>	<b>17</b>
<b>2.1. Introduction</b>	<b>17</b>
<b>2.2. Data protection officers</b>	<b>17</b>
<b>2.3. Prior checks</b>	<b>18</b>
2.3.1. Legal base	18
2.3.2. Procedure	19
2.3.3. Quantitative analysis	20
2.3.4. Main issues in ex post cases	24
2.3.5. Main issues in proper prior checks	26
2.3.6. Consultations on need for prior checking and notifications not subject to prior checking	27
2.3.7. Follow-up of prior check opinions and consultations	27
2.3.8. Conclusions and future	28
<b>2.4. Complaints</b>	<b>29</b>
2.4.1. Introduction	29
2.4.2. Cases declared admissible	30
2.4.3. Cases not admissible: main reasons for inadmissibility	32
2.4.4. Collaboration with the European Ombudsman	33
2.4.5. Further work in the field of complaints	33
<b>2.5. Inquiries</b>	<b>33</b>
<b>2.6. Administrative measures</b>	<b>35</b>
<b>2.7. Public access to documents and data protection</b>	<b>36</b>
<b>2.8. E-monitoring</b>	<b>36</b>
<b>2.9. Eurodac</b>	<b>37</b>

<b>3. Consultation</b>	<b>39</b>
<b>3.1. Introduction</b>	<b>39</b>
<b>3.2. Consultation policy</b>	<b>39</b>
3.2.1. Implementation of consultation policy	39
3.2.2. Inventory	40
<b>3.3. Opinions on legislative proposals</b>	<b>41</b>
3.3.1. General remarks	41
3.3.2. Horizontal issues	41
3.3.3. Individual opinions	42
<b>3.4. Other activities</b>	<b>46</b>
<b>3.5. New developments</b>	<b>48</b>
3.5.1. Technological developments	48
3.5.2. New developments in policy and legislation	50
<b>4. Cooperation</b>	<b>53</b>
<b>4.1. Article 29 Working Party</b>	<b>53</b>
<b>4.2. Council Working Party on Data Protection</b>	<b>54</b>
<b>4.3. Third pillar</b>	<b>55</b>
<b>4.4. European conference</b>	<b>56</b>
<b>4.5. International conference</b>	<b>57</b>
<b>5. Communication</b>	<b>59</b>
<b>5.1. Introduction</b>	<b>59</b>
<b>5.2. Main activities and target groups</b>	<b>60</b>
<b>5.3. Website</b>	<b>61</b>
<b>5.4. Speeches</b>	<b>62</b>
<b>5.5. Newsletter</b>	<b>63</b>
<b>5.6. Press service</b>	<b>63</b>
<b>5.7. Information or advice</b>	<b>64</b>
<b>5.8. EU Open Day</b>	<b>65</b>
<b>6. Administration, budget and staff</b>	<b>67</b>
<b>6.1. Introduction: developing the new institution</b>	<b>67</b>
<b>6.2. Budget</b>	<b>67</b>
<b>6.3. Human resources</b>	<b>68</b>
6.3.1. Recruitment	68
6.3.2. Traineeship programme	69
6.3.3. Programme for seconded national experts	69
6.3.4. Organisation chart	69
6.3.5. Training	69
<b>6.4. Administrative assistance and interinstitutional cooperation</b>	<b>70</b>
6.4.1. Extension of the administrative cooperation agreement	70
6.4.2. Follow-up of interinstitutional cooperation	70
6.4.3. External relations	71
<b>6.5. Infrastructure</b>	<b>71</b>

<b>6.6. Administrative environment</b>	<b>71</b>
6.6.1. Follow-up of the establishment of internal control standards	71
6.6.2. Setting up a Staff Committee	71
6.6.3. Flexitime	71
6.6.4. Internal rules	72
<b>6.7. Objectives for 2007</b>	<b>72</b>
Annex A — Legal framework	73
Annex B — Extract from Regulation (EC) No 45/2001	75
Annex C — List of abbreviations	77
Annex D — List of data protection officers (DPO)	78
Annex E — Prior checking handling time per case and per institution	79
Annex F — List of prior check opinions	81
Annex G — List of opinions on legislative proposals	86
Annex H — Composition of the EDPS Secretariat	88
Annex I — List of administrative agreements and decisions	90



# User guide

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

Chapter 1 (Balance and perspectives) presents a general overview of the activities of the EDPS. This chapter also highlights results achieved in 2006 and puts forth objectives for 2007.

Chapter 2 (Supervision) extensively describes the work done to ensure and monitor the EC institutions' and bodies' compliance with their data protection obligations. A general overview is followed by the role of the Data Protection Officers (DPO) in the EU administration. This chapter includes an analysis of prior checks, complaints and inquiries and advice on administrative measures dealt with in 2006. It also addresses a memorandum of understanding signed with the European Ombudsman, and gives a follow-up to the paper on transparency and public access, published in July 2005. Moreover, it includes a section on e-monitoring and an update on the supervision of Eurodac.

Chapter 3 (Consultation) deals with developments in the EDPS's advisory role, focusing on opinions issued on legislative proposals and related documents, as well as on their impact in a growing number of areas. The chapter also contains an analysis of horizontal themes and introduces some new technological issues, such as the role of enabling technologies and R & D for privacy and data protection.

Chapter 4 (Cooperation) describes work done in key forums such as the Article 29 Working Party, in the joint supervisory authorities of the 'third pillar', and at the European as well as the International Data Protection Conference.

Chapter 5 (Communication) presents the 'London Initiative' and runs through the use of different communication tools, such as the website, newsletters, the press service and speeches.

Chapter 6 (Administration, budget and staff) contains the main developments within the organisation, including budget issues, human resources questions and administrative agreements.

The report is completed by Annexes, which contain an overview of the relevant legal framework, extracts of Regulation (EC) No 45/2001, a list of abbreviations, statistics for prior checks, the list of DPOs of institutions and bodies and the composition of the EDPS secretariat, etc.

A separate executive summary has been published for those who prefer the short version of the main developments of 2006.

Those wanting to find out more about the EDPS are encouraged to visit our website which remains our primary tool of communication: [www.edps.europa.eu](http://www.edps.europa.eu). The website also contains a subscription feature to the bi-monthly newsletter.

Paperback copies of the annual report as well as the executive summary may be ordered free of charge; the contact details can be found on our website.

## 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 EC institutions and bodies process personal data. The EDPS is responsible for:

- monitoring and ensuring that the provisions of Regulation EC (No) 45/2001, as well as other Community acts on the protection of fundamental rights and freedoms, are complied with when EC institutions and bodies process personal data ('supervision');
- advising the EC 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 '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 EC legislation and policies, whenever relevant;
- improve the quality of EU policies, whenever effective data protection is a basic condition for their success.



## Foreword



I have the pleasure to submit a third annual report on my activities as 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 286 of the EC Treaty.

This report covers 2006 as the second full year of activity in the existence 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 Community institutions and bodies.

After the first steps in the building of a new institution and the development of its roles at Community level, to monitor and ensure the application of legal safeguards for the protection of the personal data of citizens of the European Union, it is now time to start measuring the results.

This report shows that there has been substantial progress in 2006 in different fields. The EDPS has been recognised as a new authoritative and visible player in a highly relevant area. The majority of EU institutions and bodies are well on their way in making the data protection rules and principles work in daily practice. The advisory role of the EDPS is increasingly called upon and its impact is beginning to make a positive difference.

At least two challenges are still ahead. The first one involves the implementation of data protection rules and principles in the whole EU administration and to develop a 'data protection culture' as a part of 'good governance'. The EDPS will start to take stock of progress made in all institutions and bodies as from spring 2007 and will ensure appropriate feedback.

The second challenge is to accomplish an integration of data protection principles in Community legislation, and to improve the quality of EU policies, whenever effective data protection is a basic condition for their success. It is clear that this also involves an effective integration of privacy perspectives in some areas — such as public security and law enforcement policies — that sometimes seem to be at a different course.

Let me therefore take this opportunity, once again, to thank those in the European Parliament, the Council and the Commission who continue to support our work, and many others in different institutions and bodies who are most directly responsible for the way in which data protection

is 'delivered' in practice. Let me also encourage those who will be involved in dealing with the challenges ahead.

Finally, I want to express special thanks — also on behalf of Joaquín Bayo Delgado, the Assistant Supervisor — to our members of staff who take part in our mission. The qualities that we have enjoyed in the staff have been outstanding and have contributed greatly to our growing effectiveness.

*Peter Hustinx*  
*European Data Protection Supervisor*

# 1. Balance and perspectives

## 1.1. General overview of 2006

The legal framework within which the European Data Protection Supervisor (EDPS) acts <sup>(1)</sup> has resulted in a number of tasks and powers, which allow a basic 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 Community institutions and bodies <sup>(2)</sup> comply with existing legal safeguards whenever they process personal data;
- a 'consultative' role, to advise Community 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 '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 2006 are presented. The crucial importance of information and communication about these activities has led to a separate emphasis on communication in Chapter 5. Most of these activities rely on effective management of financial, human and other resources, as will be discussed in Chapter 6.

<sup>(1)</sup> See overview of legal framework in Annex A and extract from Regulation (EC) No 45/2001 in Annex B.

<sup>(2)</sup> The terms 'institutions' and 'bodies' of Regulation (EC) No 45/2001 are used throughout the report. This also includes Community agencies. For a full list, visit the following link: [http://europa.eu/agencies/community\\_agencies/index\\_en.htm](http://europa.eu/agencies/community_agencies/index_en.htm)

It has been a deliberate choice of the EDPS to associate 'data protection' with other relevant subjects and practical results. This is why it was emphasised from the outset that many EU policies depend on the lawful processing of personal data, and that effective protection of personal data, as fundamental value underlying EU policies, should be seen as a condition for their success. The EDPS will continue to act in this general spirit and expects a positive response in return.

There has been substantial progress in 2006 in different important areas to realise this perspective. However, there needs to be more adequate progress in 2007 and beyond, along the same lines, for it to fully substantiate. The EDPS will start to take stock of progress made, with different kinds of checks for all institutions and bodies, as from spring 2007. He will also make sure that appropriate feedback is given.

## 1.2. Results in 2006

The annual report 2005 mentioned that the following main objectives had been selected for 2006. Most of these objectives have been realised.

- **Support of the DPO network**

The number of DPOs increased after publication of the EDPS' position paper on the role of DPOs in ensuring effective compliance with Regulation (EC) No 45/2001. The EDPS continued to give strong support to their network and organised a workshop for new DPOs. Bilateral evaluations of progress on notifications in large institutions are taking place at regular intervals.

- **Continue prior checking**

Prior checking of existing processing operations has also increased significantly, now including both priority and other categories. Opinions have been published on the website. The relevant policies and main issues dealt with have been shared with DPOs at regular meetings, and have been described in this annual report. A separate policy paper has therefore not been issued.

- **E-monitoring and traffic data**

A final version of the paper with guidelines on processing of personal data related to the use of electronic communication networks has been prepared for publication early in 2007. The first opinions on prior checks in this field have been issued. The EDPS will initiate procedures for evaluation of data-retention lists, when they are submitted.

- **Guidelines for personal files**

The EDPS has launched a survey on present practices concerning personal files on staff in institutions and bodies. On the basis of its results and the analysis of prior checks in related matters, a paper with guidelines is being prepared. Conservation of data on disciplinary measures has been studied and will lead to recommendations for a general practice.

- **Transfer to third countries**

Data transfers to third countries and international organisations have been analysed in a preliminary paper and discussed with OLAF. Both the need for a structural approach in line with Regulation (EC) No 45/2001 and the use of memoranda of understanding and other flexible mechanisms have been taken into account. The position of other EU bodies has also been considered.

- **Supervision of Eurodac**

An in-depth security audit of Eurodac's central database is presently being conducted with results by mid-2007. The EDPS is developing close cooperation with national data protection authorities on a system of joint supervision, with a view to building and sharing experience of other large-scale databases. A first joint report is expected in mid-2007.

- **Advisory role on legislation**

The policy paper on the advisory role of the EDPS on legislative proposals from 2005 has been implemented. The number of opinions issued has doubled and they cover a wide variety of subjects. A first inventory of rel-

evant subjects for 2007 has been published on the website. Opinions issued receive a systematic follow-up.

- **Interventions in court cases**

The EDPS has been granted the right to intervene in three cases before the Court of First Instance on public access and data protection and has taken part in the public hearing of one of them. He has also asked for intervention in the case before the Court of Justice on the validity of Directive 2006/24/EC on data retention. Court cases which raise issues for the interpretation of data protection principles are closely monitored.

- **Second version of website**

A completely revised website was launched in January 2007. Online access to the register of prior-checking notifications and a few other functionalities will be added in spring 2007. The website is now structured according to the main roles of the EDPS and provides better access to relevant information on different activities.

- **Development of resources**

The EDPS continued to develop the necessary resources and infrastructure to ensure an effective execution of his tasks. The administrative agreement concluded in 2004 with the Commission, the Parliament and the Council has been extended for another three years. The office space has been enlarged and now occupies another floor. A staff committee is taking active part in discussions.

### 1.3. Objectives for 2007

The following main objectives have been selected for 2007. The results achieved on them will be reported next year.

- **Scope of DPO network**

The network of data protection officers should reach its full scope, with all institutions and bodies taking part in its activities. The EDPS will continue to give strong support and guidance to the development of DPO functions and will encourage an exchange of best practice.

- **Continue prior checking**

The EDPS intends to finalise prior checking of existing processing operations for all relevant categories.

Special attention will be given to interinstitutional systems and other situations of joint use by institutions and bodies, with a view to streamlining and simplifying procedures. Results of prior checks will be widely shared with DPOs and other relevant parties.

- **Inspections and checks**

The EDPS will start measuring progress in the implementation of Regulation (EC) No 45/2001, with different kinds of checks for all institutions and bodies, including on-the-spot, as from spring 2007. Attention will be given to notifications and prior checks, as well as to implementation of opinions issued before in prior checking cases. The EDPS will also develop and publish a more general inspection policy.

- **Video-surveillance**

The EDPS will develop and issue guidelines for video-surveillance by institutions and bodies, with a possible impact on the privacy of staff and visitors. The guidelines will cover the use of video-surveillance as such and the conditions for privacy-compliant video-surveillance practices.

- **Horizontal issues**

Opinions on prior checks and decisions on complaints have addressed a number of common issues, which are also useful for other institutions and bodies than those involved in these cases. The EDPS will develop papers on such horizontal issues and make them widely accessible as guidance for all institutions and bodies.

- **Consultation on legislation**

The EDPS will continue to issue opinions on proposals for new legislation and ensure adequate follow-up. This advisory role will cover a wider area of subjects and be built on a systematic inventory and selection of relevant subjects and priorities. Special attention

will be given to relevant proposals for implementing decisions.

- **Data protection in third pillar**

The EDPS will continue to give special attention to the development and timely adoption of a general framework for data protection in the third pillar. He will also closely follow proposals for exchange of personal data across borders or to provide access to private or public sector data for law enforcement purposes.

- **Communicating data protection**

The EDPS will give strong support to follow-up activities of the 'London Initiative' (see paragraph 5.1) aiming at 'communicating data protection and making it more effective'. This involves activities from 'raising awareness' to 'better implementation' and 'effective enforcement' of data protection principles.

- **Rules of procedure**

With the perspective and experience gathered so far, the EDPS will adopt rules of procedure covering his different roles and activities, and make them widely accessible. These rules will be supplemented by practical information and tools for interested parties, such as persons considering submitting a complaint or a request for advice, and institutions or bodies subject to an inspection.

- **Resource management**

The EDPS will further improve the management of financial and human resources, by a renewal of the budget structure, adoption of internal rules in relevant areas, such as evaluation of staff, and development of a training policy. Different improvements will also be implemented in the internal office environment, including electronic mail handling and information security.



## 2. Supervision

### 2.1. Introduction

The task of the European Data Protection Supervisor (EDPS) is to supervise in an independent manner processing operations carried out by Community institutions or bodies that either completely or partially fall within the scope of Community law (except the Court of Justice acting in its judicial capacity). The regulation describes and grants a number of duties and powers, which enable the EDPS to carry out his supervisory task.

Prior checking has continued to be the main aspect of supervision during 2006. This task involves scanning the activities of the institutions and bodies in fields which are likely to present specific risks for data subjects, as defined in Article 27 of Regulation (EC) No 45/2001. As explained below, checking processing operations already in place, together with those being planned, gives an accurate picture of the processing of personal data in the institutions and bodies. The EDPS' opinions

allow controllers to adapt their processing operations to the guidance of the EDPS, especially where the non-compliance with the data protection rules may seriously endanger the rights of individuals. The EDPS also has other methods at his disposal such as the handling of complaints and inquiries.

As regards the powers vested in the EDPS, no order, warning or ban has been issued so far. To date, it has been sufficient for the EDPS to express his views (in prior checks as well as on complaints) in the form of recommendations. Controllers have implemented those recommendations or expressed the intention of doing so and are taking the necessary steps. The promptness of the responses differs from one case to another. The EDPS has developed a systematic follow-up of the recommendations.

### 2.2. Data protection officers

The regulation provides that at least one person should be appointed as Data Protection Officer (DPO) (Article 24.1). 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) and a 'data protection coordinator' (DPC) in each one of the other directorates-general, in order to coordinate all aspects of data protection in the DG.

For a number of years, the DPOs have met at regular intervals in order to share common experiences and discuss horizontal issues.



Assistant Supervisor Joaquín Bayo Delgado during a meeting with staff.



EDPS attending a meeting of the DPO network in Lisbon, Portugal.

This informal network has proved productive in terms of collaboration. This has continued during 2006.

The EDPS has attended a part of each of the meetings held between the DPOs in March (Court of Justice, Luxembourg), in June (EMCDDA, Lisbon) and in October (EDPS, Brussels). These meetings were a good occasion for the EDPS to update the DPOs on his work and to discuss issues of common interest. The EDPS used this forum to explain and discuss the procedure for prior checks and some of the main concepts of the regulation relevant to the prior checking procedure (e.g. controller, processing operations). It also afforded the EDPS the opportunity to outline the progress made in dealing with prior checking cases and to give details on some of the findings resulting from prior checking work (see below 2.3.). This collaboration between the EDPS and the DPOs has thus continued to develop in a very positive manner.

Back-to-back with the June meeting in Lisbon, a workshop for the new DPOs was organised by the EDPS with the help of some experienced DPOs. The main points of the regulation were analysed, focusing mainly on the practical issues which could help new DPOs to develop their tasks.

In November 2006, a new forum of collaboration between the EDPS and the DPOs started, namely the setting-up of a working group on time limits for conservation of data, on blocking and on erasure. The Assistant EDPS and two staff members as well as some DPOs are meeting regularly to produce a paper that

can be of practical guidance on those subjects for controllers and IT experts.

During 2006, the EDPS insisted on the legal obligation of all institutions and bodies to appoint a DPO and pointed out the key messages of his position paper on DPOs issued in 2005. As a result, seven new DPOs were appointed <sup>(3)</sup>. In this respect, it has to be reminded that the appointment by itself does not suffice and does not automatically imply full compliance with the regulation. Part-time DPOs must have enough time to devote to data protection and all of them need to have enough resources to fulfil their duties. They must also be notified more adequately of personal data processing within their institution or body and, where appropriate, notify the EDPS of any processing operations which entail specific risks for the people concerned and which therefore need to be prior checked.

## 2.3. Prior checks

### 2.3.1. Legal base

#### General principle: Article 27(1)

Article 27(1) of the regulation provides that all 'processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of

<sup>(3)</sup> Not counting vacancies in existing positions, for example because of changing to another post.

their nature, their scope or their purposes' are to be subject to prior checking by the EDPS. Article 27(2) of the regulation contains a list of processing operations that are likely to present such risks. This list is not exhaustive. Other cases not mentioned could pose specific risks to the rights and freedoms of data subjects and hence justify prior checking by the EDPS. For example, any personal data processing operation that touches upon the principle of confidentiality, as set out in Article 36, implies specific risks that justify prior checking by the EDPS. Another criterion, adopted in 2006, is the presence of some biometric data other than photographs alone, as the nature of biometrics, the possibilities of inter-linkage and the state of play of technical tools, may produce unexpected and/or undesirable results for data subjects.

#### Cases listed in Article 27(2)

Article 27(2) lists a number of processing operations that are likely to present specific risks to the rights and freedoms of data subjects:

- (a) processing of data relating to health and to suspected offences, offences, criminal convictions or security measures (*sûreté* in French, i.e. measures adopted in the framework of legal proceedings);
- (b) processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct;
- (c) processing operations allowing linkages, not provided for pursuant to national or Community legislation, between data processed for different purposes;
- (d) processing operations for the purpose of excluding individuals from a right, benefit or contract.

The criteria developed in the two previous years<sup>(4)</sup> 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 of prior checking (see also paragraph 2.3.6.).

### 2.3.2. Procedure

#### Notification/consultation

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

#### Period, suspension and extension

The EDPS must deliver his opinion within two months following the receipt of the notification. Should the EDPS make a request for further information, the period of two months is usually suspended until the EDPS has obtained it. This period of suspension days includes the time (normally seven calendar days) given to the DPO of the institution/body for comments — and further information if needed — on the final draft.

If the complexity of the matter so requires, the initial two-month period may also be extended for a further two months by decision of the EDPS which must be notified to the controller prior to the expiry of the initial two-month period. 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. Up until now, this case of a tacit opinion has never arisen.

#### Register

Article 27(5) of the regulation provides that the EDPS must keep a register of all processing operations of which he has been notified for prior checking. This register must contain the information referred to in Article 25 and be open to public inspection.

The basis for such a register is a notification form to be filled in by DPOs and sent to the EDPS. The need for further information is thus reduced as much as possible.

In the interest of transparency, all information is included in the public register (except for the security measures which are not mentioned in the register) and is open to public inspection.

Once the EDPS has delivered his opinion, it is made public. Later on, the changes made by the controller in the light of the EDPS opinion are also mentioned in summary form. In this way, two goals are achieved. On the one hand, the information on a given processing operation is kept up to date and, on the other, the transparency principle is complied with.

All this information will be made available on the new website of the EDPS, together with a summary of the case.

<sup>(4)</sup> See annual report 2005, paragraph 2.3.1.

## Opinions

Pursuant to Article 27(4) of the regulation, 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 concerned.

Opinions are structured as follows: a description of proceedings; a summary of the facts; a legal analysis; conclusions.

The legal analysis starts with an examination of whether the case actually qualifies for prior checking. As mentioned above, if the case does not fall within the scope of the cases listed in Article 27(2), the EDPS will assess the specific risk to rights and freedoms of the data subject. Once the case qualifies for prior checking, the core of the legal analysis is an examination of whether the processing operation complies with the relevant provisions of the regulation. Where necessary, recommendations are made to the effect of ensuring compliance with the regulation. In the conclusion, the EDPS has so far normally stated that the processing does not seem to involve a breach of any provision of the regulation, provided that the recommendations issued are taken into account. In two opinions issued in 2006 (2006-301 and 2006-142), the conclusions were different: the processing operations were in breach of the regulation and some recommendations had to be implemented to bring them into compliance.

A case manual has been drafted to guarantee, as in other areas, 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 to opinions, based on accumulated practical experience and is continuously updated. It also includes a checklist.

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 paragraph 2.3.7.)

### 2.3.3. Quantitative analysis

#### Distinction of *ex post* cases and proper prior checking cases

The regulation came into force on 1 February 2001. Article 50 provides that Community institutions and

bodies needed to ensure that processing operations which were then already underway were brought into conformity with the regulation within one year of that date (i.e. by 1 February 2002). The appointment of the EDPS and the Assistant EDPS entered into effect on 17 January 2004.

Prior checks concern not only operations not yet in progress ('proper' prior checks), but also processing operations that started before 17 January 2004 or before the regulation came into force (*ex post* prior checks). In such situations, an Article 27 check could not be 'prior' in the strict sense of the word, but must be dealt with on an *ex post* basis. With this pragmatic approach, the EDPS makes sure that Article 50 of the regulation is complied with in the area of processing operations that present specific risks.

In order to deal with the backlog of cases likely to be subject to prior checking, the EDPS requested the DPOs to analyse the situation of their institution concerning processing operations within the scope of Article 27. Following the receipt of contributions from all DPOs, a list of cases subject to prior checking was made and subsequently refined.

As a result of the inventory, some categories were identified in most institutions and bodies and therefore found suitable for a more systematic supervision. To allow for the most efficient use of the human resources available, the EDPS prioritised the work on *ex post* prior checking cases, setting the following priority categories:

1. medical files (both *stricto sensu* and containing health-related data);
2. staff appraisal (including also future staff (recruitment));
3. disciplinary procedures;
4. social services;
5. e-monitoring.

These prioritisation criteria apply only to *ex post* cases, as proper prior checking cases must be dealt with before the processing operation is implemented, following the plans of the institution or body.

### Opinions on prior checking cases issued in 2006

In 2006, 54 opinions <sup>(5)</sup> on prior checking notifications were issued.

Council	13 prior checking cases (12 opinions)
Commission	12 prior checking cases
Central Bank	5 prior checking cases (4 opinions)
Court of Justice	5 prior checking cases
Investment Bank	5 prior checking cases
Parliament	4 prior checking cases (3 opinions)
CdT <sup>(6)</sup>	3 prior checking cases
EPSO <sup>(7)</sup>	3 prior checking cases
Court of Auditors	2 prior checking cases
Committee of Regions	1 prior checking case
Economic and Social Committee	1 prior checking case
EUMC <sup>(8)</sup>	1 prior checking case
OHIM <sup>(9)</sup>	1 prior checking case
OLAF <sup>(10)</sup>	1 prior checking case

Those 57 cases represent an increase of 67.6 % of work in prior checking compared with 2005. This workload will increase with no doubt in 2007 (see below).

Out of the 57 prior checking cases (54 opinions), only five were proper prior checking cases, i.e. the institutions concerned (Court of Auditors for one of them, Commission for three and Parliament for the fifth) followed the procedure involved for prior checking before implementing the processing operation. Two of those five prior checking cases were related to evaluation, one to e-monitoring and two to other themes such as the sharing of a database online among European delegations in China or the independence of financial actors. The remaining 52 cases were *ex post* prior checking cases.

In addition to these 57 prior checking cases on which an opinion has been issued, the EDPS has also dealt with nine cases which were found not to be subject to prior checking: five notifications came from the Commission, one from the Economic and Social Committee (ECSC) and Committee of the Regions (CoR) (which share some infrastructures), one from the EUMC and two from the Parliament — all of them on various matters such as, for example, the Internal Auditing Service (IAS), e-voting or internal audit service (Commission), user account management, standards for the use of IT systems and services (EUMC) and streamline (Parliament). See also paragraph 2.3.6.

### Analysis by institution/body

Most institutions and bodies have notified processing operations likely to present specific risks. The EDPS has fixed a deadline, spring 2007, to complete all notifications of *ex post* prior checking.

Agencies deserve a specific comment. In 2005, only one agency (OHIM) notified some cases. The EDPS had assumed that many other agencies would notify processing operations in the near future, but this has not been the case. Only two other agencies sent notifications on processing operations, the EUMC and the Translation Centre, the latter with two notifications on the evaluation area and one regarding sick leave. The EDPS is really expecting more notifications from agencies as some of them, newly established, have already announced their own inventory and notifications to come, such as EMEA <sup>(11)</sup> and EMCDDA <sup>(12)</sup>. Some other agencies have started to notify processing operations; the related opinions will be issued in 2007 (see below 'Notifications for prior checking received before 1 January 2007 and pending').

<sup>(5)</sup> The EDPS received 57 notifications but for practical reasons and due to the fact that some cases were linked to same purposes, six notifications (two of the ECB, two of the Council and two of the Parliament) were treated jointly. This is why 57 notifications were received and 54 opinions were issued.

<sup>(6)</sup> Translation Centre for the Bodies of the European Union.

<sup>(7)</sup> European Personnel Selection Office (which relies on the DPO of the Commission).

<sup>(8)</sup> European Monitoring Centre on Racism and Xenophobia.

<sup>(9)</sup> Office for Harmonisation in the Internal Market.

<sup>(10)</sup> European Anti-Fraud Office.

<sup>(11)</sup> European Medicines Agency.

<sup>(12)</sup> European Monitoring Centre for Drugs and Drug Addiction.

### Analysis by category

The number of prior checking cases dealt with, by category of priority, is as follows:

Category one (medical files)	14 prior checking cases
Category two (staff appraisal)	23 prior checking cases
Category three (disciplinary procedures)	4 prior checking cases
Category four (social services)	2 prior checking cases
Category five (e-monitoring)	5 prior checking cases
Other areas	9 prior checking cases

Category one includes the medical file itself and its different contents (11 prior checking cases) and all procedures linked to allowances or sickness schemes (three prior checking cases). This priority is nearly stable in percentage (26.5 % of cases in 2005, 24.6 % of cases in 2006) but the number of cases has increased significantly, showing that the institutions and bodies are aware of the need of a prior check.

The major category theme remains the second one, relating to the evaluation of staff (23 files out of the 57), even if the percentage is decreasing (56 % of cases in 2005, 40.4 % in 2006). The appraisal concerns all staff members of the European Community, including officials, temporary agents and contractual agents, including recruitment procedures. Not only selection and evaluation procedures have been notified, but also certification and attestation procedures. It should be added that those 23 files include the three major notifications of EPSO (respectively relating to recruitment of officials, of temporary agents and contractual agents) which deal with the recruitment system set up for all the EU institutions.

Regarding the third category (disciplinary procedures), only four files were sent, by the ECB <sup>(13)</sup>, the ECJ <sup>(14)</sup> and the Council. The 'major institutions' have all fulfilled their obligation regarding this category, except the EESC and the CoR. Some agencies such as OHIM and EMCDDA have announced the sending of those notifications.

Regarding the fourth category (social services), there are only two files, concerning the Council and the Commission. Those two notifications were very well developed and documented. Notifications on this cat-

egory have already been received from the Parliament and the Court of Justice but the EDPS opinions will be issued in 2007. Other notifications are of course expected.

The fifth category (e-monitoring) has been a major aspect of the EDPS work in 2006. A paper is about to be published, after a complex survey among institutions and bodies and a special seminar devoted to the matter. Meanwhile, only proper prior checks were carried out. Already five files were notified by the institutions (Commission (2), ECB, EIB and Council). And many others are already scheduled for 2007.

Regarding the notifications of *ex post* cases which do not belong to those priority categories, they could be divided in two groups. Some are related to financial matters such as PIF (Financial Irregularities Panel, Commission), the Early Warning System (Commission and Court of Justice), call for tenders (Committee of Regions), procurement procedure (Court of Justice) and independence of financial actors (Parliament). The others are various, relating to the EU–China Tourism Agreement (Commission), to the participation in a strike (Commission), or to internal investigations (OLAF). These various notifications have been an opportunity for the EDPS to set up criteria in very sensitive areas, such as the Early Warning System and the internal investigations of OLAF (see paragraph 2.3.4).

### Work of the EDPS and the institutions and bodies

The two charts in Annex E illustrate the work of the EDPS and of the institutions and bodies. They detail the number of working days of the EDPS, the number of extension days required by the EDPS and the number of suspension days (time needed to receive information from the institutions and bodies).

*Number of working days of the EDPS per prior check:* this represents an increase of only 4.4 %, or 2.5 days more of work than in 2005 (55.5 days in 2005 and 57.9 in 2006). This remains a satisfactory figure considering the increasing complexity of the notifications sent to the EDPS.

*Number of extension days for the EDPS:* this represents an increase of 62.6 % but in absolute terms only two days more than in 2005 (3.3 days in 2005 and 5.4 days in 2006). It is due mainly to the complexity of

<sup>(13)</sup> European Central Bank.

<sup>(14)</sup> European Court of Justice.

three specific files: the file on internal investigations of OLAF, the file on the Early Warning System of the Commission (with important changes during the period during which the EDPS was preparing his opinion) and the file on recruitment of contractual agents by EPSO (with a major new database being set up too during EDPS' work). In the two first cases, a special meeting with the controller and the DPO was needed.

*Number of suspension days:* since mid-2006, this includes the suspension for seven or 10 days for comments and further information from the DPO on the final draft. The increase between 2005 (average of 29.8 days by file) and 2006 (average of 72.8 days by file) is 144.1 %. This covers very different situations. In fact, the EDPS unfortunately has to underline that three files were suspended for the very long periods of 236, 258 and 276 days respectively.

Even if some circumstances may explain that kind of delay, the EDPS regrets these figures. Institutions and bodies should make an effort to reduce the time needed to send the information. In any case, the EDPS once again reminds the institutions and bodies of their obligation to cooperate with the EDPS and to provide him with the requested information, according to Article 30 of the regulation.

*Average by institutions:* the charts show that many institutions and bodies have increased their number of suspension days very significantly; some others in a lesser manner, such as the Council. The EDPS would like to mention that the Commission and the Court of Auditors have decreased their numbers of suspension days (respectively – 39.3 % and – 45.2 %). Hopefully, the other institutions and bodies will follow this direction.

### Notifications for prior checking received before 1 January 2007 and pending

The year 2007 will be a time during which the EDPS expects a lot of notifications, as the institutions and bodies will tend to comply with the deadline of 'spring 2007'. By the end of 2006, 26 prior checking cases were already in process. Of these, one notification was sent in 2005 and 25 notifications in 2006 (nine in December), and 11 were notified in January 2007. Two of these have been considered as not subject to prior checking. One is a true prior checking case

('incompetence', notification of the Court of Auditors, opinion already issued on 18 January 2007).

OLAF	5 prior checking cases
Parliament	4 prior checking cases
European Commission	3 prior checking cases
European Central Bank	3 prior checking cases
EESC and COR	2 prior checking cases
European Investment Bank	2 prior checking cases
Court of Auditors	1 prior checking case
CPVO <sup>(15)</sup>	1 prior checking case
European Court of Justice	1 prior checking case
EFSA <sup>(16)</sup>	1 prior checking case
EPSO	1 prior checking case
ETF <sup>(17)</sup>	1 prior checking case
Translation Centre (CdT)	1 prior checking case

### Analysis by institution and body

The EDPS welcomes that four agencies (CdT, ETF, EFSA and CPVO) have started to send their notifications and encourages the other agencies and bodies to do the same. The specific case of OLAF is underlined below.

### Analysis by category

The number of notified prior checking cases by category of priority is as follows:

Category one (medical files)	4 prior checking cases
Category two (staff appraisal)	8 prior checking cases
Category three (disciplinary procedures)	none
Category four (social services)	2 prior checking cases
Category five (e-monitoring)	6 prior checking cases
Other area	6 prior checking cases <sup>(18)</sup>

In category one, there has been a continuing process of notifications. Among them, the EDPS received (from three institutions), the notification of medical files *stricto sensu*, that is, files held by medical services. This is expected to continue in 2007, as many procedures involve medical files. The EDPS welcomes that

<sup>(15)</sup> Community Plant Variety Office.

<sup>(16)</sup> European Food Safety Authority.

<sup>(17)</sup> European Training Foundation.

<sup>(18)</sup> Related to call for tenders (Commission) and five notifications from OLAF about the administrative, financial, judicial and disciplinary follow-up and about monitoring cases.

notifications in this area are being received from the Commission <sup>(19)</sup> in early 2007. PMO <sup>(20)</sup> should follow; as it has already been seen (see 2.4.2).

The second category theme (staff appraisal) still represents the majority of cases — eight out of 26 files (30.8 %). Major cases have been notified within this area (EPSO cases, see above) which concern all institutions and bodies, but the EDPS would like to underline that some institutions have not notified their own procedures about the use of the reserve lists of EPSO.

Regarding the third category (disciplinary procedures), the EDPS is expecting notifications from the institutions, especially from agencies and the two committees.

Concerning category four (social services), two notifications have already been received (one from the Parliament and one from the Court of Justice).

Category five (e-monitoring) is still of particular importance. As mentioned above, the paper on e-monitoring is being used as background for the prior checking of e-monitoring systems and serves as reference for prior checking in this domain (see paragraph 2.7). Many institutions and bodies are concerned in this area where six opinions have been issued: the Commission, the ECB (two), the EIB (two) and the Council. The EESC and COR notified that kind of procedures. The ECB and the EIB notified other processing operations in that category.

The other area involves, in particular, OLAF, which is in the course of notifying many prior checking cases due to their specific and sensitive area of working. Those notifications have been the first consequence of the joint analysis and planning by OLAF's DPO and the EDPS team to allow smooth work. This process of notification will continue to increase. OLAF has already notified seven prior checking cases in January 2007 and 20 more are expected before 1 March 2007.

#### 2.3.4. Main issues in ex post cases

*Medical data and other health-related data* are processed by the institutions and bodies. Any data relating to direct or indirect knowledge of the state of health of an individual fall under this category. Therefore, sick leaves and sickness insurance claims are subject to prior checking.-

As already mentioned above, 11 prior checking cases directly linked to the medical file itself and their different aspects have been supervised by the EDPS. The Council sent the medical file itself for prior checking. The EDPS made numerous recommendations, notably on the quality of data, on data retention and information to be given to the data subject. With all of the prior checking cases (Council, ECB and EIB), and also the pending ones on the same subject (Parliament, EESC and COR), the EDPS has a good overview.

*Staff evaluation* is a common processing operation in all institutions and bodies for obvious reasons. EPSO plays a major role in this area. The EDPS received the notifications on the recruitment of officials, of temporary agents and of contractual agents. In all these cases, EPSO has substantially followed the principles of the regulation, although the EDPS made some recommendations regarding the retention time and long-term conservation and on limiting transmission only to services in charge of recruitment. A specific recommendation regarded the need to publish, as a general rule, the conditions of competitions and, specifically, the fields of evaluation in the oral test and their detailed marks, and the right of access of candidates accordingly. For the contractual agents' recruitment, among other recommendations, the EDPS pointed out the need not to limit the right of access to the results or to suppress the merit groups in the lists of successful candidates to be used by recruiting institutions. The EDPS also addressed recommendations on the conservation period of data kept in electronic format.

Another important prior checking case was the EU-CV online (not to be mistaken with Sysper 2 e-CV; see below for main issues of proper prior checks), which replaces the current manual or semi-manual handling of spontaneous applications for Commission vacancies with a harmonised electronic system and for which the EDPS made some recommendations regarding storage periods, use of backup data and consent of the reference persons included in the CV.

---

<sup>(19)</sup> It plays an interinstitutional role on specific aspects (e.g. archiving of medical files).

<sup>(20)</sup> Office for administration and payment of individual entitlements.

Institutions such as the CdT, EESC, ECJ, EUMC, EIB and ECB sent their processing operations relating to recruitment and/or evaluation. The main recommendations relate to quality of data, right of access, information to be given and data retention. The new areas of certification procedure and attestation procedure (one was treated as a true prior checking case, see below) have also been sent to the EDPS both by the Council and the Court of Auditors; the main recommendations relate to data retention and right of information. The certification procedure from EPSO is pending.

Lastly, two prior checks refer to management of time (Council and EIB). Among others areas, recommendations relate to the data conservation period, the definition of managers' access to the personal data of the staff members under their responsibility, and to the information to be given to the data subject.

*Administrative inquiries and disciplinary proceedings:* four cases of *ex post* checking were carried out in this area. The Council, ECB (one case for each area) and the Court of Justice were the institutions involved. Recommendations were made on data retention, which remains a major issue (principle of limited conservation versus principle of prescription of sanctions), on rights of access, rectification and information, and on processing of special categories of data.

*Social services:* Social service files may include details relating to the health of an official, which subject the data processing to prior control by the EDPS. Moreover, data processing by the social welfare service may be intended to evaluate personal aspects relating to the data subjects.

Only two prior checking cases were analysed. The recommendations to the Commission were focused on the extreme care needed in all communications that include personal data with external services. Moreover, the EDPS called for data to be rendered anonymous when statistics of financial assistance are prepared; and called for the stamping of the words 'staff matter' on all letters, given the confidentiality and sensitivity of the data. The recommendations to the Council were on data quality, right of access and rectification, and information to be given.

*E-monitoring:* during 2006, awaiting the general conclusions of the paper on e-monitoring (see para-

graph 2.8), the *ex post* cases in this area dealt with the recording of telephone conversations. Indeed, it presents specific problems which are so important that a specific provision and special safeguards have been provided in Regulation (EC) No 45/2001, notably on the confidentiality of communications. As recordings are mainly used to identify violations of professional secrecy or misuse of inside information, and to identify fraud, there are further grounds for prior checking.

In the case of the Council's security and prevention telephone lines, the recommendations concern the purpose limitation, the limitation of the data subject's right of access and the information to external callers. For the ECB and EIB, the recommendations centred essentially around the obligation to provide information to counterparties to a transaction, whose data are also recorded. The EDPS also stressed the importance of determining the purposes for which the data are initially collected and ensuring that they are not subsequently processed for other, incompatible, purposes. In the case of the urgency and security telephone line of the Commission, the recommendations related basically to the information to be given to data subjects.

This area will remain an important one as six prior checking cases are already pending for 2007.

*Other areas:* the Early Warning System (EWS) and the internal investigations of OLAF should be highlighted.

The EWS system was notified by the Commission and by the Court of Justice. The principal purpose of the EWS is to ensure circulation of restricted information concerning third parties (natural or legal persons) among all Commission departments about recipients of Community funds (beneficiaries) who have committed fraud, administrative errors or irregularities and about other circumstances related to these beneficiaries who could represent a threat to the Communities' financial interests. The information may also include natural persons with powers of representation, decision-making or control over given legal persons. Other institutions do not establish their own central database, but they use the database of the Commission to exchange information with the latter (in the case of the Court of Justice).

An opinion has been issued on the EWS Commission system. Some recommendations were made regarding the possibility of publishing the Commission EWS decision in the Official Journal, the data quality, the definition and the granting of the rights of access (restriction to this right should remain an exception) and to be completed by a right of rectification in case of errors or wrong evaluation, the information to be given to data subjects and that, as a rule, the person concerned is informed of the issuance of a warning against him/her. Regarding the case of the Court of Justice, the main recommendations were about data retention policy, data quality, rights of access and rectification, and information to be given.

In order to combat financial irregularities such as fraud and corruption, OLAF has the power to conduct internal administrative investigations in the EU institutions and bodies. The investigation power also extends to serious matters of misconduct by EU staff. OLAF has access to any information of any data medium and can request oral information from staff members, etc. Where necessary, the results of its investigations are submitted to national and/or Community authorities for follow-up (for instance judicial or disciplinary). The EDPS made numerous recommendations to improve compliance with the regulation, notably on the rights of data subjects, such as access, rectification and information. The EDPS also addressed guarantees on the quality of the data to be introduced in the investigation files and on the confidentiality of e-mails, as well as on transfer of reports and related documents, etc.

### **2.3.5. Main issues in proper prior checks**

The EDPS should normally give his opinion prior to the start of a processing operation, so as to guarantee the rights and freedoms of the data subjects from the beginning. This is the rationale of Article 27. In parallel with the handling of *ex post* prior checking cases, five cases of 'proper' <sup>(21)</sup> prior checking were notified to the EDPS in 2006. Contrary to the general conclusion concerning all proper prior checking cases in 2005, during 2006 proper prior checks have been very well documented. As can be expected, procedural rules continue to be a predominant aspect of the notification.

The attestation procedure case of the Court of Auditors dealt with the new procedure allowing staff members

<sup>(21)</sup> i.e. cases concerning a not-yet-implemented processing operation.

to change grade (previous C and D grades towards AST grade). The only recommendations to improve the system from a data protection point of view were about data retention and information to be given.

The other case dealing with evaluation was the Sysper 2 e-CV of the Commission (not to be mistaken with the EU-CV online, see above), which is an information tool allowing the Commission staff to enter their professional data. The main recommendations concerned the information to be provided to staff members as well as the establishment of guarantees related to access to data in the system.

A case of e-monitoring was the voice recording of helpdesk calls of the Commission. The EDPS made numerous recommendations along two main lines to avoid unlawfulness: recording dialogues for solving IT problems should be combined with a very short storage period; the further use of recordings for training can only be admissible, either by the dialogues and related data being anonymised or if the consent of the users and the operators is obtained.

The Parliament sent a notification about the independence of financial actors. This processing is carried out by means of the evaluation questionnaires in order to be able to detect the risks of conflict of interest in the performance of sensitive duties by financial actors within the Parliament and which were likely to represent a threat to those financial interests. The main recommendations were about the guarantees on the purpose limitation and about information to be given.

An unusual notification was sent by the Commission about the EU–China Tourism Agreement Approved Destination Status (ADS). A protected website of the European Commission External Relations DG facilitates real-time exchange of information between the Commission and the embassies and consulates of European countries (EU plus some others) that participate in the ADS tourism agreement with China. The website contains a list of accredited travel agencies and their couriers (people acting on their behalf) authorised to deal with ADS visa applications to European Union countries. It contains proposed and imposed sanctions for violating the ADS rules, but also other information. The EDPS prior checked the system because sanction data on travel agencies can be data on 'suspected offences' committed by natural persons.

Excluding agencies from certain rights means excluding their couriers from those rights. The recommendations centred on the data subjects' rights of access and rectification and on the information to be given to them. Access to the website should only be given on a case-by-case basis — when necessary for Commission staff to perform their task.

### **2.3.6. Consultations on need for prior checking and notifications not subject to prior checking**

During 2006 the number of consultations on the need for prior checking by the EDPS has remained significant. Some of the cases referred to above were previously subjects of consultation as to this need: the EU–China Tourism Agreement intranet website, EIB telephone recording, EU-CV online, etc.

The legal entities file of the Commission as such was considered not subject to prior checking but some aspects, basically information to data subjects being introduced in the file, were analysed in the EWS opinion, as LEF is the database feeding and being fed by EWS.

The 'security clearance' processing of the Council was not considered needing prior check as the role of Council is not meaningful in the evaluation done by the Member State concerned.

'Outgoing paper mail checking' of the two Committees was not concluded to be prior-checkable either as it was possible to avoid any breach of confidentiality through a change in the procedure. The EDPS has followed up this change and closed the case.

The 'Adonis' system of the CoA, as that of the Commission, is not subject to prior checking due to the fact that the content of mails and e-mails is not meant to be processed, thus not falling within the scope of Article 27(2)(a).

The ECB insider trading rules case has been special in the sense that, although considered initially subject to prior checking, it has been found not to be, on the same grounds as IAS, mentioned below. The fact that internal auditors also conduct, in a given case, an inquiry on possible breach of rules by a person does not change the nature of the processing. In that case, the inquiry procedure, already prior checked, is applied.

Another category of cases has been very useful to define the scope of prior checking. Sometimes, after a careful study of the notification sent by the DPO, the EDPS finds the processing operation not subject to prior checking. In those cases, the reasons leading to that conclusion are stated, normally in a letter to the DPO, frequently with some recommendations found necessary in the course of the analysis. As the letter containing those elements replaces a formal opinion, it is felt useful to publish it on the EDPS website.

Two interesting decisions in this domain have been cases of the EESC and CoR (sharing IT infrastructure) on the e-mail system and the user account management. They presented the opportunity to clarify the conditions in which the EDPS considers e-monitoring cases to be subject to prior checking. In short, confidentiality and/or evaluation of behaviour must be at stake.

Another important case has been the notification submitted by the Commission DPO on the Internal Auditing Service (IAS). The conclusion reached is that processing operations for the purpose of auditing are not subject to prior checking as they do not intend to evaluate persons but systems; whenever doubts on behaviour of persons appear, the data must be sent to the competent investigation body. This criterion is obviously applicable also to the core activity of the Court of Auditors.

The case on 'Electronic vote — elections for the Committee of Personnel' of the Commission was the occasion to point out that not all sensitive data make prior checking necessary (only those listed in Article 27(2)(a)) and the possible malfunctioning of a system does not constitute sufficient grounds for prior checking either.

### **2.3.7. Follow-up of prior check opinions and consultations**

When the EDPS delivers the prior check opinion, a series of recommendations which must be taken into account in order to make the processing operation comply with the regulation are usually provided. Recommendations are also provided when a case is analysed to decide on the need for prior checking and some critical aspects appear to deserve corrective measures. Should the controller not comply with these recommendations, the EDPS may exercise the powers

granted to him under Article 47 of the regulation. The EDPS may, in particular, refer the matter to the Community institution or body concerned.

Furthermore, the EDPS may order that requests to exercise certain rights in relation to the data be complied with (if such requests have been refused in breach of Articles 13 to 19), or may warn or admonish the controller. He may also order the rectification, blocking, erasure or destruction of all data or impose a temporary or definitive ban on processing. Should the decisions of the EDPS not be complied with, he has a right to refer the matter to the Court of Justice of the European Communities under the conditions provided for in the EC Treaty.

All prior checking cases have led to recommendations. As explained above (see paragraphs 2.3.4 and 2.3.5), most recommendations concern information to data subjects, data conservation periods, purpose limitation and the rights of access and rectification. Institutions and bodies are willing to follow these recommendations and to date there has been no need for executive decisions. The time for implementing those measures varies from case to case. Since June 2006, the EDPS has requested, in the formal letter sent with his opinion, that the institution inform the EDPS of the measures taken to implement the recommendations within a period of three months. It should lead to the opening of a follow-up on its own initiative by the institution or body involved, which starts to be the case.

During 2006, and regarding the follow-up which could also concern opinions issued in 2005, 83 cases (among 137 notifications received between 2004 and 2006 and which represents 60.6 % of the cases) have been treated with the following repartition:

Closed cases	17 cases
Cases for which the follow-up has been launched but with no reply of the institution	17 cases
Cases for which the follow-up has been launched and is under process and/or well advanced	34 cases
Cases for which the follow-up has not yet been started as the opinions are quite recent (since October 2006)	13 cases
Specific follow-up of cases not subject to prior checking	2 cases

The follow-up launched but with no reply of the institution or body (17 cases) represents 97 recommendations of the EDPS. The follow-up under process and/or well advanced (34 cases) represents 256 recommendations of the EDPS.

In two cases, the analysis of the notification led to the conclusion that the case was not subject to prior checking but, nevertheless, 10 recommendations were made and followed up. One case is closed and the other well advanced.

In three consultations on the need for prior checking, seven recommendations were also made and followed up. One case is closed and the other two well advanced.

### 2.3.8. Conclusions and future

The year 2006 has been an intensive one as demonstrated by the above quantitative and qualitative analysis. Nevertheless, the number of prior checking cases received is below expectation, considering the deadline of spring 2007 already referred to in the annual report of 2005. The expectations for the last semester of 2006 were higher as to the number of cases to be received. An exception has been OLAF, which has notified a significant amount of cases and continues to do so. Others have increased numbers in early 2007. The priority areas are not yet covered in all institutions and bodies, so efforts have to continue to meet the deadline.

But not only priority matters have to receive attention. All *ex post* cases have to be notified, as they are also covered by Article 27 of the regulation and thus present specific risks for the rights and freedoms of data subjects.

A special area which deserved attention during 2006 will continue to do so in 2007: the interinstitutional cases subject to prior checking. In many cases, several institutions or bodies share processing operations in the fields of medical data, evaluation, promotion, etc. The respective roles differ from one case to another (one institution providing services to others, several bodies taking charge of partial aspects, etc), but all of them share the common feature of being complex. This will be given much attention in 2007.

Electronic communications also will receive special attention. *Ex post* cases in this priority area have been somewhat delayed due to the need to finalise the study leading to the e-monitoring paper (see paragraph 2.8.). All the processing operations done by institutions and bodies aiming at the monitoring of the proper use of telecommunication systems should be checked by the EDPS during 2007.

The delays in providing information requested to complete the prior checking notification have also to be improved. There are too many cases still pending, some many months old.

The year 2007 must also be one in which all agencies and bodies have a DPO. To that effect a campaign will be launched to remind, once again, of this legal obligation.

After spring, a new approach will be started in parallel with the ongoing work on prior checks. Inspections will begin, including on-the-spot inspections if necessary. The aim will be to make sure that the process of notifications has included all cases under Article 27, as well as compliance with the regulation in other cases of personal data processing.

## 2.4. Complaints

### 2.4.1. Introduction

Article 41(2) of Regulation (ECa) No 45/2001 provides that the EDPS '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'. Part of this monitoring is carried out by the handling of complaints as provided for in Article 46(a) <sup>(22)</sup>.

Any natural person may lodge a complaint to the EDPS with no conditions of nationality or place

of residence <sup>(23)</sup>. Complaints are only admissible if they emanate from a natural person and concern the breach of data protection rules by an EU institution or body when processing personal data in the exercise of activities all or part of which fall within the scope of Community law. As we will see below, a number of complaints filed to the EDPS were declared inadmissible because they were outside the area of competence of the EDPS.

Whenever the EDPS receives a complaint, he sends an acknowledgement of receipt to the complainant without prejudice to the admissibility of the case, unless the complaint is clearly inadmissible without need for further examination. The EDPS will also request that the complainant inform him on other possible actions before a national court, the European Court of Justice or before the Ombudsman (whether pending or not).

If the case is admissible, the EDPS will proceed to inquire about the case, notably by contacting the institution/body concerned or by requesting further information from the complainant. The EDPS has the power to obtain from the controller or the institution/body access to all personal data and to all information necessary for the inquiry and obtain access to any premises in which a controller or institution/body carries on its activities. As will be seen below, the EDPS has made use of these powers when handling complaints in 2006.

In the event of an alleged breach of data protection law, the EDPS can refer a matter to the controller concerned, and make proposals for remedying the breach or improving the protection of the data subjects; the EDPS can order the controller to comply with requests to exercise certain rights of the data subject; he can warn or admonish the controller; he can order the rectification, blocking, erasure or destruction of all data; the EDPS can impose a ban on processing; he can refer the matter to the Community institution concerned, or to the EP, the Council and the Commission. Lastly, the EDPS can refer a matter to the Court of Justice <sup>(24)</sup>.

<sup>(22)</sup> According to Article 46(a) the EDPS shall 'hear and investigate complaints, and inform the data subject of the outcome within a reasonable period'.

<sup>(23)</sup> According to Article 32(2) 'every data subject may lodge a complaint to the EDPS if he or she considers that his or her rights under Article 286 of the Treaty have been infringed as a result of the processing of his or her personal data by a Community institution or body'. Article 33: 'Any person employed with a Community institution or body may lodge a complaint with the EDPS regarding an alleged breach of the provisions of Regulation (EC) No 45/2001, without acting through official channels.'

<sup>(24)</sup> See Article 47(1) of Regulation (EC) No 45/2001.

Should the decision involve the adoption of measures by the institution/body, the EDPS follows this up with the institution/body concerned.

Fifty-two complaints were received by the EDPS in 2006. Of these 52 cases, only 10 were declared admissible and further examined by the EDPS. These are briefly examined below.

#### 2.4.2. Cases declared admissible

##### Information made public on lobbyists

A complaint was made against the European Parliament (2006-95) concerning the possible publication of the home addresses of accredited lobbyists. The application form for a lobbyist badge implied that it was compulsory to fill in the home address. Further on in the form, it was mentioned that the information that followed would not be made public, thereby implying that previous information — including the private home address — would be published.

The EDPS found that no other information than the name of the lobbyist and the organisation that he/she represents was made public. A recommendation to amend the application form to reflect the practice was therefore made, and the European Parliament updated their form accordingly. The EDPS also stated that publishing the private home addresses of lobbyists would undermine their privacy.

However, more information could be made public, as long as the lobbyists would be informed of it when their data are collected <sup>(25)</sup>.

##### Access to medical report and transfer of medical data

A former official of the EC made a complaint against the PMO (Pay Master Office) on two aspects which he felt were not complying with the regulation (2006-120 and 390). One concerned the right of access to a medical report. The EDPS, after revision of the initial

decision, concluded that the temporary limitation, while the report was not final, was lawful, but advised that access should be granted to the final report in the usual manner as to other reports of the same kind and that the access to the interim report should be reconsidered in view of the final report. The second aspect was the transfer of medical data to an insurance company without the consent of the complainant. The conclusion was that the transfer was necessary and non-excessive in the context of the duties of the EC administration to insure the financial consequences



The number of surveillance cameras has increased during recent years.

of professional sickness, early retirement, etc. In any case, the processing of medical data by the PMO has to be submitted for prior checking. The revision of this second decision has also been asked and is currently pending. Some other issues were raised on access to documents under Regulation (EC) No 1049/2001.

##### Complaint on an investigation

A complaint was made against the European Economic and Social Committee (EESC) (2006-181 and 287) concerning the initial phase of the investigation requested by an official on unauthorised access to his

<sup>(25)</sup> See findings available on the website: [http://www.edps.europa.eu/EDP-SWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/06-08-31\\_transparency\\_lobbyists\\_EN.pdf](http://www.edps.europa.eu/EDP-SWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/06-08-31_transparency_lobbyists_EN.pdf)

e-mail account (alleged use of his user-id and password) and the subsequent failure of the HR director to provide access to the complainant's log files in order to prove this unauthorised access. Due to an initial misunderstanding as to what was needed to investigate the unauthorised access (the IT service concluded that access was to the log files of a third party rather than that of the data subject himself), the EESC initially concluded that the investigation could not take place and informed the complainant of such a conclusion. Following the request of intervention made by the complainant to the DPO of the EESC, the access to and analysis of the complainant's own log files provided indicia of unauthorised access to the complainant e-mail boxes. In his decision on this case, the EDPS concluded that it was regrettable that, until the introduction of a formal complaint by the complainant and the intervention of the Committee's DPO, the Committee's administration, due to the misunderstanding referred to above and lack of adequate technical and legal analysis, failed to come to a satisfactory conclusion regarding the request of the complainant.

### **Video-surveillance**

An EU citizen launched a complaint against the European Parliament (EP) concerning its video-surveillance practices (2006-185). The complainant challenged the proportionality of surveillance outside EP buildings in Brussels. He also claimed that the notice provided to the public was insufficient. In its decision, the EDPS required the EP to improve the notice provided to the public and to adjust the positioning of the surveillance cameras. The main focus of the EDPS was to ensure that demonstrators are not monitored by the EP, either purposefully, or incidentally, as this could have an inhibiting effect on free speech. During the follow-up to his opinion, the EDPS continued to work with the EP to improve its video-surveillance practices taking into account the special security needs of the EP, including securing visits of Heads of States or other VIPs requiring increased protection, which were not addressed in the initial EDPS decision. In connection with the complaint, the EDPS also initiated a survey among the EU institutions and bodies, and commenced work on a set of video-surveillance guidelines, which is planned to be finalised during 2007.

### **Access to an investigation report**

A complaint was made against the Court of Auditors concerning a person's right of access under Article 13 to an investigation report (2006-239). This report concerned an alleged case of harassment and bad management following an Article 90 complaint under the Staff Regulations. One of the parties concerned requested access to the report, but this was refused to him by the Court on the basis that he was 'a person not concerned about the report'. The EDPS endeavoured in this case to examine the scope of a person's right of access under Article 13 and possible limitations to this right under Article 20. The handling of the case included an on-the-spot visit by the Assistant Supervisor and a member of his team notably to gain access to the content of this report and the reports on interviews carried out by the investigator. The EDPS issued a decision in which he found that the complainant is entitled to have access to any outcome of the inquiry which concerns him. The only exceptions should be where data reveals information not related in any way to the complainant and the outcome of reports with witnesses. The EDPS therefore requested that the Court of Auditors give further, although not complete, access to the investigation report to the complainant. The implementation is still pending.

### **Right of access and rectification**

A complaint was introduced against the Directorate-General for Personnel and Administration of the European Commission claiming a right of access under Article 13 to certain documents concerning the complainant and the right to rectify certain data under Article 14 (2006-266). The complaint also invoked Article 18 to object to the processing of the complainant's data. After further requests for clarification of the situation, the EDPS concluded that the administration had provided access to all the documents required to the exception of one e-mail for which the administration did not detain enough information to identify the document. As concerns the exercise of the right of rectification, the EDPS reiterated his position that the right of rectification cannot be applied to subjective data on grounds of inaccuracy. Finally, as concerns the possibility of objecting to the processing on the basis of Article 18 of the regulation, the EDPS considered that the complainant failed to invoke 'compelling legitimate grounds'.

### **Right of rectification and blocking**

One complaint (2006-436) concerned the right to rectification without delay of incomplete data (Article 14) of the career history (*historique de carrière*) in Sysper2 (information system of the European Commission in the area of HR which includes several sub-modules). Though the Commission contested the claim of incomplete data, it was proposed to introduce a field for comments in the complainant's career history. The EDPS accepted the proposal as a temporary solution, and in addition requested explanations as to the technical difficulties concerning the right to rectification of career history data in Sysper2. Both the interim solution and the explanations are pending.

### **Complaint against an investigation by a DPO**

A complaint was received against an investigation carried out by a data protection officer (2006-451). The investigation by the DPO followed a request for access to a recalled e-mail. The complainant questioned whether this investigation was within the competence of the DPO, whether the procedure followed by the DPO was in conformity with the law and whether the measures adopted by the DPO respected the principles of proportionality, good faith and due diligence. After carrying out an investigation into the facts of the case, and requesting further clarifications from the parties concerned, the EDPS concluded that the launching of the investigation was to be considered as lawful not only because the DPO could base his action on powers granted in the annex to the regulation, but also because the investigation was triggered by a request for access under Article 13 of the regulation. However the EDPS considered the complaint as founded as the measures adopted by the DPO were excessive in the light of the interests at stake and the possibility of using other less intrusive means. The DPO has asked for revision and comments from the complainant are pending.

### **Publication in annual report 2005**

One additional complaint arose in the context of the follow-up to a case mentioned in the annual report 2005 (2005-190), and subsequently pursued by complainant in a complaint to the European Ombudsman. The complainant also objected to the brief presentation of his case in the annual report 2005, stating that it had been incorrect and premature. The EDPS

rejected the complaint. This aspect is now also before the European Ombudsman.

### **2.4.3. Cases not admissible: main reasons for inadmissibility**

Out of the 52 complaints received in 2006, 42 were declared not admissible for reason of lack of competence of the EDPS. This constitutes a two-fold increase compared to 2005. The vast majority of these complaints do not concern personal data processing by an EC institution or body; but they concern exclusively processing on a national level. Some of these complaints asked the EDPS to reconsider a position taken by a national data protection authority; which falls outside of his mandate. The complainants were informed that the European Commission would be competent in the event of a Member State failing to implement Directive 95/46/EC correctly.

Three cases concerned processing of personal data of EC staff members, although the substance of the complaints was not on the processing done by an institution or body. The complaints thus involved entities of the EU administration that need to comply with Regulation (EC) No 45/2001, although the alleged data protection breaches concerned processing on the national scene. One such example was a staff member complaining about having received political information to his office address from a party in relation to elections in the Member State of his origin. In that case, it could not be excluded that the office address was provided by the institution to the permanent representation of the Member State. However, the complaint was about a political party, acting under national law, having used this information. Therefore, contact details of national data protection authorities were provided, along with an explanation of why the EDPS was not competent to deal with the case.

The high number of inadmissible complaints, particularly as to issues on the national level, has resulted in more explicit information on the new website as to the scope of the EDPS' competence. This subject has also turned out to be relevant for petitions to the European Parliament on data protection issues, which are sometimes referred to the EDPS for comments or advice. If the issue is exclusively on the national level or does not involve the processing of personal data by a Community institution or body, the EDPS is not

competent in the matter and can only provide general information allowing the Petitions Committee to decide on an appropriate course of action.

#### 2.4.4. Collaboration with the European Ombudsman

According to Article 195 of the EC Treaty, the European Ombudsman is empowered to receive complaints concerning instances of maladministration in the activities of the Community institutions or bodies. The European Ombudsman and the EDPS have overlapping competences in the area of complaint handling in the sense that instances of maladministration may concern the processing of personal data. Therefore, complaints lodged with the Ombudsman may involve data protection issues. Likewise, complaints brought before the EDPS may concern complaints which have already been, partially or totally, the object of a decision by the Ombudsman.



Peter Hustinx, P. Nikiforos Diamandouros and Joaquín Bayo Delgado, after the signing of the memorandum of understanding.

In order to avoid unnecessary duplication and to ensure to a maximum extent a consistent approach to both general and specific data protection issues raised by complaints, a memorandum of understanding was signed in November 2006 between the European Ombudsman and the EDPS. Both parties notably undertake to inform complainants about the other institution when this could be relevant to them and facilitate the transfer of complaints; to inform the other institution about complaints relevant to it; not to reopen a complaint that has already been

brought forward, unless significant new evidence is submitted and to adopt a consistent approach to the legal and administrative aspects of data protection, thereby promoting the rights and interests of citizens and complainants <sup>(26)</sup>.

#### 2.4.5. Further work in the field of complaints

The EDPS has continued working on the drafting of an internal manual for complaint handling by EDPS staff. The main elements of the procedure and a model form for the submission of complaints, with information on the admissibility of complaints, will be made available on the website in due course.

The Assistant Supervisor and a member of staff attended the national data protection authorities' case-handling workshop in Madrid in March 2006. During this workshop the Assistant Supervisor gave a presentation on prior checking by the EDPS. Three members of staff also attended a similar workshop in Athens in October 2006 and gave a presentation on the video-surveillance survey carried out by the EDPS.

## 2.5. Inquiries

During 2006, the EDPS conducted a number of inquiries in different areas, a few of which merit special attention in this report.

### European Commission's Competition DG

Further to a letter received from a data protection authority in one of the Member States, a preliminary inquiry was conducted in relation to the European Commission's large-scale inquiry carried out in the electricity sector (2005-2007).

The Commission had sent different formats of questionnaires to various kinds of electricity companies based in 23 Member States. Since the data protection authority's letter suggested that personal data

<sup>(26)</sup> ( The MoU available at: [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/News/06-11-30\\_EO\\_EDPS\\_MoU\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/News/06-11-30_EO_EDPS_MoU_EN.pdf)

were unlawfully collected in the framework of the Commission's sector inquiry, the EDPS carried out a preliminary inquiry: requesting and analysing the questionnaires, conducting an on-the-spot visit and meeting with staff at the Competition DG for clarifying some aspects of the information processing in the Commission's inquiry.

On the basis of his initial findings, the EDPS requested the DG to ensure that personal data would not be processed in the Commission's inquiry, and recommended specific measures to this effect. In November 2006, Competition DG presented a report on the implementation of a series of actions, along the lines suggested by the EDPS, and including detailed checks on data collected and providing specific information to its staff. Further to this report, ensuring that no personal data relating to electricity consumers were, nor will be processed in the course of the Commission's enquiry in the electricity sector, the EDPS decided to close his preliminary inquiry in this case.

### **SWIFT**

In 2006, the EDPS initiated an inquiry on the transfers of European citizen's banking data to US authorities through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (2006-357).

After the news on this issue broke in the media in June 2006, the EDPS sent a letter to the European Central Bank, asking for information on its role as a user as well as an overseer of SWIFT. Furthermore, the EDPS took part in a hearing organised by the European Parliament in October and actively contributed to the opinion adopted by the Article 29 Working Party in November.

In October, the EDPS had a meeting in Frankfurt with the President of the European Central Bank, with a view to exchanging further information on the state of play of the EDPS' inquiry and to get additional information on the role of the ECB. In December, after receiving further relevant documents and factual information from both SWIFT and the ECB, the EDPS sent his draft opinion to the ECB for comments.

After carefully analysing the ECB's comments, the EDPS adopted his final opinion early in 2007. The opinion deals with the different roles played by the ECB in this case. As a SWIFT customer, the ECB,

being a joint controller together with SWIFT, should ensure full compliance with Regulation (EC) No 45/2001 with regard to its payment operations. As overseer, jointly with other central banks, the ECB should promote that oversight on SWIFT includes data protection and that confidentiality rules do not prevent relevant authorities from being timely informed when necessary. Finally, the EDPS called on the ECB to use its central role as policymaker with a view to ensuring that European payment systems are compliant with European data protection law.

During 2007, the EDPS will closely monitor the developments of this case with a view to ensuring that payment operations of Community institutions are carried out in full compliance with the data protection regulation. In a broader perspective, the EDPS, in cooperation with other national data protection authorities, will keep using his consultative role in order to ensure that the architecture of European payment systems does not impinge on the privacy of EU banks' customers.

### **Other inquiries**

As mentioned in paragraph 2.4.2, the Assistant Supervisor and a member of his team also carried out an investigation in the frame of a complaint against the Court of Auditors (2006-239). This on-the-spot visit enabled the Assistant Supervisor to gain access to the full report of which access had been partly refused to the complainant.

An on-the-spot visit to the video-surveillance control room of the European Parliament was also made in the framework of the complaint on video-surveillance against the European Parliament (2006-185).

The EDPS is working on rules of procedure as provided for under Article 46(k) of Regulation (EC) No 45/2001. These will include some provisions on inquiries and will be adopted shortly.

The EDPS is also working on an inspection policy with the aim of establishing a framework and methodology for his inspections. Information on existing standards of inspections has been gathered from national data protection authorities and from other EU institutions serving as input for this work. The initial focus of the inspection policy of the EDPS will be compliance by spring 2007 in the field of appointment of a DPO in

Community institutions and bodies, and notification for prior checking. The policy will subsequently be broadened to monitoring full compliance with Regulation (EC) No 45/2001.

## 2.6. Administrative measures

The regulation provides for a right of the EDPS to be informed about administrative measures which relate to the processing of personal data. The EDPS may issue his opinion, either following a request from the institution or body or on his own initiative. Article 46(d) reinforces this mandate when it comes to implementing rules of the regulation and especially those concerning the data protection officers (Article 24(8)).

On his own initiative, as foreseen in the annual report 2005, the EDPS has launched a survey on present practices concerning personal files on staff in institutions and bodies. With its results and those of the analysis of prior checks in related matters, a paper with guidelines is being prepared. At the same time, the specific problem of the conservation of data on disciplinary measures has been studied in the context of the present provisions of the Staff Regulations and some suggestions for a general practice are being drafted.

As also foreseen in last year's report, data transfers to third countries and international organisations, namely by OLAF, have been discussed and a preliminary paper drafted. Both the need for a structural approach, with a pragmatic interpretation of Article 9(8) of Regulation (EC) No 45/2001 and the use of memoranda of understanding, and the unavoidable use of exceptions in Article 9(6), with possible safeguards, have been taken into account.

As mentioned above in paragraph 2.4.2, a complaint has triggered the launching of a survey on video-surveillance in the European institutions and bodies. After receiving information from their DPOs, information on best practice is being gathered from national supervisory authorities. With all this material, guidelines on the use of video-surveillance will be issued.

As to advice on request, during 2006 the ECB sent its draft implementing rules of the regulation for advice (2006-541). The EDPS recommended adding value to the text of the regulation itself, by detailing the DPO's

powers and tasks, the exercise of data subjects' rights, notifications, etc. He welcomed the prior consultation of the EDPS before the appraisal of the DPO and suggested to include the Assistant DPO.

Many other administrative measures were the object of consultation and comments by the EDPS.

A very meaningful one has been the consultation by the Chair of the College of the Heads of Administration on a draft note about the conservation delay for medical data (2006-532). The EDPS opinion has been issued early in 2007, underlining the need to change the general time limit from minimum to maximum and to set several shorter periods for specific cases, without prejudice of some exceptions beyond the maximum 30 years period (asbestos, etc.).

The DPO of the Commission sought advice on the applicability of Article 9 of the regulation (transfer of personal data to non-EU countries and organisations) (2006-403) following the Lindqvist case<sup>(27)</sup>. The EDPS opinion is that Article 9 does not apply to the publishing of personal data via the Internet by European institutions and bodies, but the rest of provisions of the regulation do apply, preventing the Internet from being a way to circumvent data protection principles in the transfer of personal data.

The same DPO asked for an opinion on applicability of the regulation to activities under the Euratom Treaty (2006-311). The answer was affirmative.

The DPO of the European Parliament consulted on the use of video-surveillance for purposes other than security and without recording (2006-490 and 2006-510). The conclusions were that the regulation applies provided personal data are processed (i.e. images of identified or identifiable persons). Some guidance on best practices was given.

The DPO of the Court of Auditors consulted on the best way to comply with Article 13 of the regulation (right of access) as concerns data subjects whose data have been collected by the Court but are not object of an actual auditing case as they were not randomly chosen for such operation (2006-341). A practical solution, and yet respectful with the regulation, was advised.

<sup>(27)</sup> Judgment of the European Court of Justice of 6 November 2003 (C-101/01).

The DPO of the European Court of Justice asked the opinion of the EDPS on his analysis on the publication on the Intranet of the reserve lists of contractual agents (2006-122). His conclusions on the need to give proactive information and the right to object, among others, were confirmed.

The DPO of the Council consulted the EDPS on the processing of personal data of attendees to the Council's working groups (2006-125). Some recommendations on information and data conservation were made.

A variety of other matters were the subject of consultations from the same and other DPOs, for example, access to IT data, withdrawal of consent, data subjects in harassment investigations, e-mail archiving, etc.

## 2.7. Public access to documents and data protection

The background paper on public access to documents and data protection which was published in July 2005 received broad support among the institutions and bodies which are usually subject to both Regulation (EC) No 1049/2001 and Regulation (EC) No 45/2001. The European Commission has a different interpretation of the key provision — Article 4(1)(b) of Regulation (EC) No 1049/2001 — and does not therefore use the findings of the paper in its daily work.

The bottom line of the paper is that there can be no automatic refusal to documents held by the EU administration just because they contain personal data. The 'Article 4(1)(b) exception' <sup>(28)</sup> of the public access regulation stipulates that the privacy of a person needs to be undermined for disclosure to be hindered. Urging for a concrete and individual examination in each case, the paper puts the carefully worded exception into context by arguing that the following criteria must be met for the non-disclosure of a public document:

1. the privacy of the data subject must be at stake;
2. public access must substantially affect the data subject;

---

<sup>(28)</sup> The institutions shall refuse access to a document where disclosure 'would undermine the protection of [...] privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data'.

3. public access is not allowed by the data protection legislation.

After having intervened in a relevant case before the Court of First Instance (T-194/04; *Bavarian Lager v. Commission*) <sup>(29)</sup>, the EDPS participated in the hearing before the Court in September. The case dates back to 1996, when the European Commission held a meeting which addressed the conditions for importing beer to the UK. A company wanting to sell German beer in the UK requested access to the list of participants of the meeting. That was refused by the Commission, which based itself mainly on data protection legislation for the non-disclosure.

The Court hearing constituted a good opportunity for the EDPS to explain and present the conclusions of the paper — i.e. that documents containing personal data can be made public unless it substantially harms the privacy of the individual. Because data protection rules do not imply that there is a general right to participate anonymously in Commission activities, the EDPS intervened in support of the applicant. Stressing that transparency and data protection are two fundamental rights, on equal footing, the EDPS asked the Court to annul the Commission's refusal to disclose the attendance list in full. The Court has not yet pronounced its judgment.

Further involvement of the EDPS in this area included:

- advising the European Ombudsman in complaints on the topic;
- providing the Secretariat of the Article 29 Working Party with an analysis of whether information about recipients of the Fisheries Fund could be disclosed;
- dealing with a complaint on whether the home address of lobbyists accredited to the European Parliament could be disclosed (see also paragraph 2.4.2).

## 2.8. E-monitoring

The use of electronic communication tools within the EU institutions and bodies generates personal data, the processing of which triggers the application of Regula-

---

<sup>(29)</sup> The EDPS also intervened in two other cases before the Court of First Instance where the same issues are raised (cases T-170/03 and T-161/04). These cases have not yet reached the stages of hearing.

tion (EC) No 45/2001. At the end of 2004, the EDPS started work on the processing of data generated by the use of electronic communications (telephone, e-mail, mobile phone, internet, etc.) in the EU institutions and bodies. A draft 'e-monitoring' paper on the use and monitoring of the communications network was circulated amongst the DPOs in March 2006 in order to collect their comments and reactions.

To test the guiding principles of the document, the EDPS organised a workshop in June 2006. Over 50 representatives of the EU administration participated, ranging from DPOs, data protection coordinators and IT staff, to staff committees. After a general presentation of the main conclusions of the document, the EDPS tested these and a set of guidelines to concrete scenarios. The participants worked on themes such as the conservation of traffic data for budget purposes; the reading of staff e-mails during their absence and the employer's monitoring of the fair use policy.

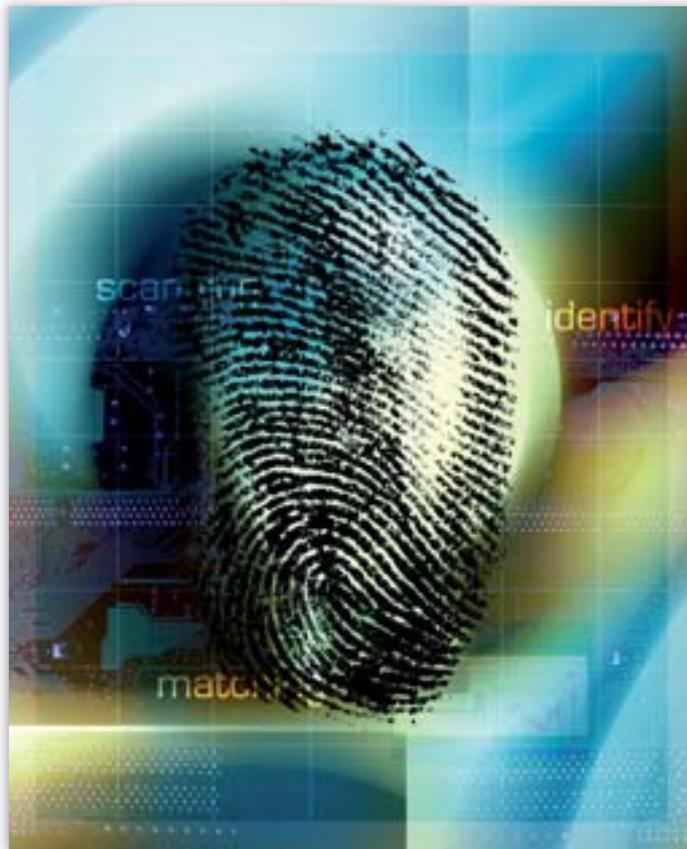
Building on the outcome of the workshop and comments made following it, the final document is being made ready for publication early in 2007.

## 2.9. Eurodac

Eurodac is a large database of fingerprints of applicants for asylum and illegal immigrants found within the EU. The database helps the effective application of the Dublin Convention on handling claims for asylum. The EDPS is the competent authority that monitors the activities of Eurodac's Central Unit, in order to ensure that the rights of data subjects are not violated. Another essential aspect of the EDPS' supervisory role is the cooperation with national supervisory authorities to:

- examine implementation problems in connection with the operation of Eurodac;
- examine possible difficulties encountered by national supervisory authorities during checks;
- draw up recommendations for common solutions to existing problems.

In view of these responsibilities, regular meetings and informal contacts between the EDPS and Commission services have taken place to discuss different aspects of EDPS' supervisory tasks. These contacts concerned in particular the inspection of Eurodac carried out by the EDPS and the concerns about the high number of 'special searches' performed in the system <sup>(30)</sup>.



The Eurodac system contains more than 250.000 fingerprints.

The Commission and the European Parliament also wanted to see this issue clarified. It has been one of the main objectives of the cooperation with national data protection authorities to investigate and, if needed, correct the situation.

<sup>(30)</sup> Reflecting the data protection rules to safeguard the rights of the data subject to access his/her own data, Article 18 paragraph 2 of the Eurodac regulation provides for a possibility to conduct 'special searches' on request of the person concerned whose data are stored in the central database. This category of transactions has been used extensively by some states; the figures did not match the actual number of requests for access made by individuals. This raised the question of their actual use.

The EDPS has also taken into consideration the annual report published by the Commission concerning the operation of Eurodac<sup>(31)</sup> and the statistics published by the Commission concerning the use of the system.

### **Supervision of the Central Unit**

In 2005, the EDPS carried out an inspection of security and data protection situation at Eurodac's Central Unit. The EDPS inspected the Eurodac premises (Central Unit and Business Continuity System) and submitted a set of questions. In his report, issued in February 2006<sup>(32)</sup>, the EDPS made a series of recommendations with the aim of improving the system.

The second phase of the Eurodac supervision — an in-depth security audit — started at the end of September 2006. It aims at evaluating the efficiency of the implemented security and data protection measures. In application of Regulation (EC) No 2004/46, the EDPS requested ENISA (European Network and Information Security Agency) to provide contacts with national experts in the Member States and to deliver advice on the methodology of the security audit. An audit team consisting of EDPS, German and French experts, has been set up. Based on a detailed and interactive presentation of the system and the situation given by the Eurodac helpdesk, the audit team adopted the IT-Grundschutz methodology developed by the BSI<sup>(33)</sup> (Bundesamt für Sicherheit in der Informationstechnik) in order to conduct this audit under the mandate of the EDPS. The final report of the audit is expected in the spring of 2007.

### **Cooperation with national supervisory authorities**

The EDPS and national data protection authorities met in 2005 to establish a first coordinated approach to supervision: some specific issues would be investigated at national level (amongst them, the 'special searches') and the result of these investigations would be presented in a common report. These national investigations have been conducted in the course of 2006 in most of the countries that participate in the Eurodac system.

On 28 June 2006, the EDPS organised a second coordination meeting for the national data protection authorities regarding the joint supervision of Eurodac. Representatives of data protection authorities from all Member States (and Iceland and Norway) participating in the system as well as observers from Switzerland were present. The EDPS gave an outline of the state of play in Eurodac supervision from the different stakeholders' perspectives. Underlining that the so-called 'special searches' were under scrutiny by different institutions, the EDPS also mentioned that a review of the Eurodac regulation was foreseen in the near future. If needed, the group could present amendments to the regulation. The EDPS presented the findings of his first inspection of the Eurodac Central Unit, and announced that a larger audit of the Central Unit would follow.

National investigations, launched after the first coordination meeting, were addressed and some very interesting findings were shared. EDPS staff also had bilateral contacts with different national data protection authorities, either to provide guidance in the national investigation or to address the specific situation of different participants (new members, members or observers with a special status such as Norway or Switzerland).

### **What to expect in 2007?**

The year 2007 should see the completion of different activities in both areas of supervision. The security audit and the final report on coordinated national supervision are to be completed. This should coincide with the overall evaluation of the Dublin system, including Eurodac, which the Commission is to produce in the context of the first phase of the European asylum policy. The data protection aspects covered by the EDPS supervision should contribute to the assessment of the added value provided by Eurodac, while ensuring that data protection remains a priority on the agenda of the different stakeholders.

---

<sup>(31)</sup> Commission staff working document: Third annual report to the Council and the European Parliament on the activities of the Eurodac Central Unit, SEC(2006)1170.

<sup>(32)</sup> Inspection report of the European Data Protection Supervisor on the Eurodac Central Unit, Brussels, 27 February 2006.

<sup>(33)</sup> <http://www.bsi.de/>

## 3. Consultation

### 3.1. Introduction

The year 2006 was the second full year of functioning of the EDPS, and also for his duties as advisor to the Community institutions on proposals for legislation (and related documents). It was an important year in which the EDPS faced an increase in his activities and in which he further developed and improved his performance. This was seen in three key areas.

The consultation policy was further developed. In December, an inventory of the intentions for 2007 was published on the website. It consists of an introductory part, including a short analysis of the most important trends and risks as well as the priorities for 2007. It also contains an annex of the most relevant European Commission proposals that have been adopted or are programmed and that (may) require a reaction by the EDPS.

The output in terms of number of opinions increased and they now also show a wider variation in subjects. The EDPS issued 11 opinions in 2006. This almost represents twice the number of opinions issued the previous year. These opinions also reflect the relevant subjects on the policy agenda of the Commission, the European Parliament and the Council. The EDPS presented opinions on the exchange of information under the principle of availability, in the field of visas (including access to the large-scale Visa Information System (VIS)), passports and consular instructions, and on financial matters.

On a number of occasions, the EDPS used other instruments for interventions in external developments that relate to his work. This concerned, inter alia, the notion of interoperability, the developments on the transfer of passenger data following the PNR-judgment of the Court of Justice <sup>(34)</sup>, retention of traffic data, the finalisation of the legal framework for the second generation Schengen information system and negotiations in the Council on the proposal for a framework decision on the protection of personal data in the third pillar.

Finally, this chapter will not only look back to the activities in 2006, but will also look ahead. It will describe consequences for the EDPS of new technological developments as well as of new developments in the field of policy and legislation.

### 3.2. Consultation policy

#### 3.2.1. Implementation of consultation policy

The policy paper 'EDPS as an advisor to the Community institutions on proposals for legislation and related documents' <sup>(35)</sup> lays down the main elements of how the EDPS envisages fulfilling the tasks that have been assigned to him under Article 28(2) and 41 of Regulation (EC) No 45/2001.

<sup>(34)</sup> Judgment of the Court of 30 May 2006, *European Parliament v Council of the European Union* (C-317/04) and *Commission of the European Communities* (C-318/04), Joined cases C-317/04 and C-318/04, ECR [2006], Page I-4721.

<sup>(35)</sup> Published in March 2005; available on the website: <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/21>

The implementation of the policy paper during 2006 is mainly articulated by the output: the opinions mentioned in Section 3.3 and the other activities mentioned in Section 3.4. An important step forward was the inventory mentioned in Section 3.2.2.

Besides that, the following may be noted.

- European Commission services normally involve the EDPS before the formal adoption of a proposal by the Commission, quite often in parallel with its internal inter-service consultation. At this stage, the EDPS gives informal comments.
- The EDPS has also initiated informal contacts with the Council, through its Presidency and its Secretariat-General. On several occasions, the EDPS clarified and discussed his opinions within working groups of the Council dealing with the legislative proposal.
- The same activities were undertaken in relation to the LIBE Committee and other committees of the European Parliament dealing with the legislative proposal. The EDPS has initiated informal contacts with the European Parliament — with members, as well as secretariats — and he has also been available for more general discussions, such as in public hearings.
- The advisory task of the EDPS has become more and more self-evident for the institutions. The EDPS welcomes, in particular, that the Commission has developed a practice to mention the consultation of the EDPS in the preamble of its proposals. This makes the consultation of the EDPS more visible to the public.
- Special attention was given to how to advise the Commission in cases where it does not adopt a proposal (to the Council and/or the European Parliament) but decides itself. This situation applies in the case of implementing legislation by the Commission (with ‘comitology’ or not), Commission decisions declaring the adequate level of protection in a third country pursuant to Article 25(6) of Directive 95/46 or when the Commission presents a communication. In those cases, a formal opinion after the adoption by the Commission cannot influence the text of the instrument.

### 3.2.2. Inventory

An important part of the working method described in the policy paper is the selection and planning (including a regular review of it) needed in order to be effective as an advisor. The EDPS annual report for 2005 announced the establishment of priorities for the coming years, in connection with the priorities established by the Commission for 2006. This was done when the first inventory was prepared and published on the website in December 2006.

The inventory will be published every year in December and will become part of the annual work cycle. Once a year, the EDPS reports retrospectively in the annual report; once a year the prospects are provided in the inventory. The main sources of the inventory are the Commission’s work programme (normally published in October of each year) and several related planning documents of the Commission. The inventory for 2007 was prepared in close cooperation with stakeholders within the Commission.

The inventory also found a strong justification for the need to widen the scope of the consultative activities of the EDPS, which, until summer 2006, had been mainly focused on legislative documents related to the area of freedom, security and justice, as prepared within the Commission by Justice, Freedom and Security DG. The preparation of the inventory was used as an occasion to intensify the relations with the Secretariat-General of the Commission, Information Society and Media DG and the European Anti-Fraud Office (OLAF), and to establish relations with Employment, Social Affairs and Equal



Peter Hustinx during a meeting with staff.

Opportunities DG, and Health and Consumer Protection DG. All these entities have been involved in the preparation of the inventory.

The annex of the inventory which lists the most relevant Commission proposals that (may) require a reaction by the EDPS includes:

- 16 topics with high priority, on which the EDPS will issue an opinion; 20 other topics are mentioned with a lower priority and the EDPS may issue an opinion or react in another way;
- 17 legislative proposals *stricto sensu*, 19 related documents (such as communications by the European Commission) <sup>(36)</sup>;
- 11 (sets of) documents already adopted by the Commission, whilst the rest are mentioned on different programming lists.

### 3.3. Opinions on legislative proposals

#### 3.3.1. General remarks

As in 2005, the proposals in the area of freedom, security and justice (both in the first pillar relating to free movement of persons and immigration, and in the third pillar relating to police and judicial cooperation in criminal matters) constituted an important source for interventions by the EDPS. The EDPS also published a second opinion on the proposal for a Council framework decision on the protection of personal data processed in the framework of the third pillar, which is meant to establish a new and necessary building block of data protection on the level of the EU. Other important proposals with a more fundamental nature that the EDPS reacted to, include one on the organisation and content of the exchange of information extracted from criminal records between Member States, and another on the exchange of information under the principle of availability.

Moreover, proposals on ID and travel documents have been analysed by the EDPS. Proposals relating to the Community *laissez-passer* (a diplomatic passport in third countries for staff and members of the institutions who need it for their work), the uniform format for residence permits for third-country nationals and

the amendment of the common consular instructions on visas for diplomatic missions, gave the opportunity for the EDPS to underline the need of specific safeguards when biometric data are processed.

Furthermore, the EDPS advised in the areas of finance, fraud and other illegal activities affecting the Community budget. He issued two opinions concerning fraud and other illegal activities: an opinion on investigations conducted by OLAF and an opinion on mutual administrative assistance for the protection of the financial interests of the European Community against fraud and any other illegal activities. The EDPS also reacted on the proposals amending the financial regulation applicable to the general budget of the European Communities and its implementing rules.

Lastly, an opinion was issued on a proposal on enforcement of decisions and cooperation in matters relating to maintenance obligations.

#### 3.3.2. Horizontal issues

An overview of the 11 opinions leads to the following conclusions. Four opinions deal with proposals in the third pillar, three opinions find their origin in Title IV of the EC Treaty (two in the common visa policy and one in cooperation on civil law) and three opinions deal with matters outside the area of freedom, security and justice. In most cases, the EDPS supported the proposals but required specific additional data protection safeguards.

A major concern in the third pillar is the order of proposals. The EDPS opposes that legislation facilitating exchange of data is adopted before an adequate level of data protection is guaranteed. This order should be reversed. A legal framework for data protection is a *conditio sine qua non* for the exchange of personal data by law enforcement authorities, as is required by Article 30(1)(b) of the EU Treaty, and recognised in several EU policy documents. Common actions on collection, storage, processing, analysis and exchange of relevant information are subject to appropriate provisions on the protection of personal data. The legislative practice however does not comply with this requirement.

On several occasions, the EDPS addressed the issue of biometric data introduced in specific Commission proposals. Common to these interventions is that the

<sup>(36)</sup> The topics fall within the responsibility of 10 different directorates-general or similar entities within the Commission.

EDPS underlined that the introduction and processing of biometric data need to be supported by particularly consistent and strong safeguards. Biometric data are highly sensitive and present special risks in their implementation which have to be mitigated. In view of their specific characteristics, the EDPS reiterated the importance of surrounding the processing of biometric data with all the necessary safeguards. An obligation to use biometric data should only be introduced after a thorough assessment of the risks and should follow a procedure allowing full democratic control. This approach, developed in the opinion on the proposals regarding the second generation Schengen Information System (SIS II), should be applicable to any system using biometrics, whether it relates to proposals on residence permits, Community *laissez-passer* or visas for diplomatic missions.



Parts of the policy team finalising work on a legislative opinion.

Another important theme analysed in the opinions of the EDPS in 2006 refers to databases, especially the establishment and access by different authorities for specific purposes. Central databases and large-scale systems are becoming more widely used nowadays. In 2005, the EDPS analysed the legal consequences attached to the development of different large scale IT systems, and this work continued in 2006. The conclusion is that the need for such databases must be properly and carefully assessed in each case. Moreover, when such databases are established, specific data protection safeguards have to be implemented. Legal obligations that lead to substantial databases create particular risks for the data subjects, *inter alia* because of the risks of illegitimate use. The level of data protection must be equivalent, irrespective of which type of authority consults the databases.

The EDPS was repeatedly concerned about the lack of safeguards surrounding the exchange of personal data with third countries. Several proposals contained provisions for such exchanges and the EDPS stressed that mechanisms ensuring common standards and coordinated decisions on adequacy should be put in place. Exchanges with third countries should only be allowed if they ensure an adequate level of protection of personal data, or if the transfers fall within the scope of one of the derogations laid down by Directive 95/46/EC.

Finally, the quality of data was also an important horizontal theme. A high level of accuracy of data is needed to avoid ambiguity concerning the content of information processed. It is therefore important that the accuracy is regularly and properly checked. Moreover, a high level of data quality represents not only a basic

guarantee for the data subject, but also facilitates the efficient use for those who process the data.

### 3.3.3. Individual opinions <sup>(37)</sup>

#### Access to VIS by authorities responsible for internal security

The opinion of 20 January 2006 was a reaction to the proposal for a Council decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

The VIS is developed in view of the application of the European visa policy. The proposal follows directly from the establishment of the VIS — on which the EDPS issued an opinion on 23 March 2005. In that opinion, the hypothesis of access to several large-scale information and identification systems by law enforcement authorities was already envisaged. In the subsequent opinion, the EDPS supports the idea that access to the VIS by law enforcement authorities can only be granted in specific circumstances, on a case-by-case examination of the necessity and proportionality. It must be accompanied by strict safeguards. In other

<sup>(37)</sup> See the list of opinions on legislative proposals in Annex G.

words, consultation by law enforcement agencies must be limited by adequate technical and legal means to specific cases.

The opinion underlined that considerable attention has been devoted to data protection in the proposed instrument, mainly in limiting access to specific cases, and only in the framework of the fight against serious crime. However, the EDPS also underlined that, in order to grant access to third pillar authorities, the basic regulation on the VIS — a first pillar instrument — should provide for a bridging clause. The EDPS finally stressed that a coordinated approach to supervision should be ensured, also with regard to access to the VIS.

#### **Exchange of information under the principle of availability**

The principle of availability was introduced by the Hague programme in 2004 and lays down that information available to law enforcement authorities in one Member State should also be made accessible for equivalent authorities in other Member States. It is an important instrument for the development of one area of freedom, security and justice, without internal borders. The principle raises a number of data protection issues, notably because of the sensitivity of the data and the reduced control of the use of the information.

The proposal for a Council framework decision elaborates the principle into a legislative instrument. In his opinion of 28 February 2006, the EDPS analyses the proposal also in the context of other instruments that deal with the sharing of information in the combating of serious crime (such as the Prüm Convention, signed in May 2005 by seven Member States). The EDPS used the occasion to present some general points of view in the current debate.

The proposal addresses subjects such as the availability for the police in other Member States of information that is not always in the hands of the police in the Member State of origin (such as telephone data or vehicle registration data), conditions for an introduction of a system of index data, and the use of DNA-profiles for the exchange of information. In his opinion, the EDPS advocates a gradual introduction, starting with one type of data (and not six as proposed by the Commission), indirect access (index data of

information that is not available online) and a hit/no-hit system, which would allow for more control of the exchange of information than a system based on direct access. It is essential that the availability principle is complemented by appropriate data protection rules in the field of justice and police cooperation <sup>(38)</sup>.

#### **Maintenance obligations**

On 15 May 2006, the EDPS issued an opinion on the proposal for a Council regulation on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations. The proposal deals with a complex reality — maintenance payments may be awarded to children, divorced spouses, parents, etc. Those involved may live or have assets in different Member States.

The EDPS welcomes the proposal and recognises the importance of facilitating the recovery of cross-border maintenance claims within the EU. However, at the same time, data protection principles must be respected, such as purpose limitation, necessity and proportionality of data processed, limits to the use of special categories of data, storage periods and information to creditor and debtor. The most important concern of the EDPS is the key principle that data collected for a specific purpose should not be used for different purposes, which would be a consequence of the proposal. An exception to that principle can only be allowed if it is proportionate, necessary, laid down by law and foreseeable. In this respect, the proposal should provide for explicit and clear legal obligations.

#### **Criminal records**

In his opinion of 29 May 2006, the EDPS welcomed the policy choice of the proposed Council framework decision on the organisation and content of the exchange of information extracted from criminal records between Member States. However, since the framework decision for data protection in the third pillar is not yet adopted, there are no general safeguards and this leads to legal uncertainty for European citizens. Only some articles in the proposal deal with specific situations but that does not give the necessary protection. The EDPS therefore strongly recommended that it should not enter into

<sup>(38)</sup> At the time of writing it seems obvious that the framework decision as such will not be adopted. However, this does not affect the importance of the principle of availability for the exchange of law enforcement information.

force before the framework decision for data protection in the third pillar.

The specific remarks of the EDPS concern, inter alia:

- the appropriate solution with a central authority, which ensures clear responsibilities in terms of handling the information as well as in terms of supervision by the national data protection authority;
- the recommendation to make it even more clear that the convicting Member State shall be considered as the 'owner' of the personal data and that the Member State of the convicted person stores the data on the former's behalf;
- that more precise criteria for transferring personal information to a third Member State for other purposes than criminal proceedings are developed;
- that a workable language regime is needed, and that a standardised format for exchange of information is developed and implemented within less than a year.

### ***Laissez-passer***

In his opinion of 13 October 2006, the EDPS analyses the draft Council regulation on the Community *laissez-passer* (CLP) to be issued to members and staff of the institutions and used as a diplomatic passport in third countries. Introduced in the Protocol on Privileges and Immunities of the European Communities in 1965 and used since 1967, the *laissez-passer* needed to be redesigned in order to meet the current security standards for EU travel documents. The proposed new version will incorporate security elements and includes certain new categories of data, such as biometric data.

The EDPS supports the proposal, albeit with some reservations, especially concerning the use of biometric data. For instance, the EDPS reiterates his preference for the use of fallback procedures during the enrolment phase. Another concern is the possible creation of central databases containing all the biometric data contained in the CLP which would not be proportionate, according to the EDPS. Moreover, as the CLP is intended to be used in third countries, interoperability between the European systems and those of third countries must be guaranteed. In this respect, the opinion stresses that the interoperability of systems must not breach the purpose limitation principle of

the processing of data. The opinion also addresses the question of access by third countries.

Because the use of biometric data can pose risks to those staff members concerned, the EDPS has informed the institutions that the processing operation will need to be prior checked, in conformity with Article 27 of Regulation (EC) No 45/2001 <sup>(39)</sup>.

### **Residence permits**

Following the introduction of biometric features in European passports and Schengen visas, the modified proposal for a Council regulation amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, is the third proposal to rely on biometric data. The justification for the use of biometrics is that it enhances the security level and facilitates fighting illegal immigration and illegal residence.

In his opinion of 16 October 2006, the EDPS supports the proposal although stressing that the residence permit should not be seen as a travel document. Moreover, the highest security standards need to be adopted, in line with the security specifications of the Members States which are developing an e-ID card. The EDPS does not oppose the use of biometric data as long as the proper safeguards which are recommended in the opinion are implemented.

The EDPS welcomes progress made for respecting the principle of purpose limitation. However, he is concerned that the proposal does not clearly identify and define those authorities that have access to the data. The EDPS welcomes the reasoning of treating European citizens and third-country residents equally by giving them access to electronic services, such as e-government services. However, the insertion of an additional chip for such services should be postponed until a complete impact assessment study has been conducted.

### **Investigations conducted by OLAF**

An opinion on the proposal for a regulation amending Regulation (EC) No 1073/1999 concerning investigations conducted by OLAF was issued on 27 October 2006. The proposal contains revisions to most of the articles which lay down the operational rules for

---

<sup>(39)</sup> See more in paragraph 2.3, on prior checking.

those involved in OLAF investigations and, as such, it constitutes the legal basis for OLAF's operational activities. It is essential to ensure that, in doing so, the data protection and privacy rights of the persons implicated in such investigations, suspected infringers and also staff members and other individuals who provide information to OLAF, are properly guaranteed.

The proposed amendments aim at improving the effectiveness and efficiency of OLAF investigations, facilitating the exchange of information about suspected wrongdoings between OLAF and other bodies and at guaranteeing the rights of the persons implicated in an investigation, including their right to data protection and privacy. The EDPS agrees with the significance of the objectives pursued by the proposed amendments and welcomes the proposal, and in particular its procedural guarantees afforded to individuals. However, the proposal could be further improved in terms of protection of personal data without jeopardising the objectives that it pursues.

The opinion gives particular attention to the data-quality principle, the right of information, the right of access, the right of rectification and exchanges of personal information. Measures are also proposed regarding the protection and confidentiality of whistleblowers.

### **Common consular instructions**

The opinion of 27 October 2006 addressed the proposal for a regulation amending the common consular instructions on visas for diplomatic missions and consular posts and the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications. The main points of the opinion concern biometric identifiers and cooperation between consular posts in the visa procedure.

Regarding biometric identifiers, the EDPS underlines that it is a political, rather than a purely technical decision to determine from which age fingerprints shall be collected. This should not be based entirely on arguments of feasibility. The mandatory fingerprinting of all children aged 6+ especially raises ethical questions too. The EDPS moreover recalls that all biometric identification systems are inherently imperfect and that the system therefore must provide for adequate fallback solutions.

Regarding the cooperation between consular posts and embassies of Member States, the EDPS emphasises the need to guarantee data security, which can prove difficult in some third countries. When the processing of visa applications, including collecting of biometric identifiers, is outsourced to a private company, the EDPS stresses the need for it to be located in a place under diplomatic protection. Otherwise, authorities of the third State could easily access data of visa applicants and their contacts in the EU. This could prove dangerous for the visa applicants, for example in cases of political opponents trying to leave their country.

### **Mutual administrative assistance**

The amended proposal for a regulation on mutual administrative assistance for the protection of the financial interests of the European Community against fraud and any other illegal activities sets forth communication and assistance procedures between the Commission and Member States. It includes mutual administrative assistance and exchange of information.

An earlier version of the proposal in 2004 led to the adoption of the first EDPS opinion on Community legislation. In his opinion of 13 November 2006, the EDPS considered that, on the whole, the amended proposal maintains the level of protection of personal data contained in the general data protection framework of the EU. The proposal includes neither new rules on data protection nor exceptions to the existing data protection framework, but confirms the application of this legislation and in some areas calls for implementing regulations that will address data protection issues. Therefore, the real debate on data protection issues is postponed to a later stage. Since the implementing regulations will be crucial for the protection of personal data in this context, the EDPS particularly welcomed the inclusion of the obligation to consult him on the drafting of such implementing legislation.

### **Data protection in the third pillar (second opinion)**

On 29 November 2006, the EDPS issued for the first time a second opinion on a proposal for EU legislation, concerning the Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

The reason for this was two-fold. Firstly, a framework decision on the protection of personal data in the third pillar is extremely important to the EDPS. Secondly, there were serious fears that negotiations in Council would result in essential safeguards to the citizens being deleted or substantially weakened. Therefore, the EDPS recommended more time for the negotiations in order to achieve a result that offers sufficient protection.

The main concern was that the proposal in the state it was discussed in Council would lead to an artificial division in data files — between national data and data originating from another Member State. Not only would that lead to burdensome, complex and costly handling, but it would also lead to difficulties for citizens to exercise their rights. Moreover, the EDPS was concerned about the possibilities of exchanging data too with non-law enforcement authorities and private parties, the risks of not requiring an ‘adequate level of protection’ for data exchange with third countries as well as about the risk that some basic rights for data subjects, such as the right to be informed, would no longer be guaranteed. Exceptions to this right may become the rule. In December 2006, after the opinion of the EDPS, it became clear that the proposal would not be adopted and that alternatives would be sought.

### **Financial regulation**

The proposals for amending the financial regulation applicable to the general budget of the European Communities and its implementing rules are important because they affect the way in which personal data of individuals relating to financial activities are dealt with. One of the main points of the proposals is that they foresee that the Commission set up and operate a central database, common to all institutions and bodies, of candidates and tenderers under specific situations of exclusions in case of fraud, and allow the exchange of the information contained in the database with authorities at different levels.

In his opinion of 12 December 2006, the EDPS agrees with the principle of a central database in the light of the foreseen purposes of data processing. However, he underlined that a proactive approach to the rights of the data subjects should be respected. This proactive approach could consist of informing the data subjects beforehand, at the time their personal data are collected,

that these data might be made public, and of ensuring that the data subject’s right of access and right to object are respected. Furthermore, the EDPS underlined the need for specific safeguards in the light of the data protection principles for the definition of the categories of entities affected, a precise timeframe regarding the update of the information as well as an adequate security protection of the database. Moreover, in the light of the adequacy of international transfers of personal data, the EDPS insisted on providing specific safeguards in the context of transfer of personal data from the central database and on receipt of personal data from third countries and international organisations.

Finally, these proposals also gave the opportunity for the EDPS to underline the question of time limits for storage and budgetary control, for which he suggested an amendment in compliance with Regulation (EC) No 45/2001.

## **3.4. Other activities**

### **Supervision of SIS II**

On 19 October 2005, the EDPS issued an opinion on the proposals for the establishment of a second generation Schengen Information System (SIS II). One of the subjects dealt with was that supervision of the system must be ensured in a consistent and comprehensive way at both European and national levels.

In January 2006, the EDPS responded to a request from the European Parliament for advice on how the supervision of SIS II could be best structured. A meeting with representatives of the Joint Supervisory Authority for SIS resulted in a model for ‘coordinated’ supervision. This was eventually laid down in Articles 44 to 46 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) <sup>(40)</sup>. This model is now also being considered for the Visa Information System (VIS).

In March 2006, the EDPS sent a letter to the Presidency of the Council drawing its attention to the problems that might arise under European law if the management of SIS II during an interim period would

---

<sup>(40)</sup> OJ L 381, 28.12.2006, p. 4-23. See also paragraph 4.3 of this annual report.

be delegated by the Commission to one or more Member States, in particular with regard to an effective supervision of the central facilities. This resulted in a special provision in Article 47 of the regulation on data protection during the transitional period, ensuring an effective supervision by the EDPS.

### Comments on interoperability

On 10 March 2006, the EDPS issued comments on a Commission communication on interoperability of European databases. On this occasion, a somewhat lighter instrument than an opinion was chosen. These comments were, contrary to the opinions, not published in the Official Journal and not translated in all the languages of the Community. They are however publicly available on the website.

The EDPS challenges an essential point of departure of the communication, namely that 'interoperability is a technical rather than a legal or political concept'. To the EDPS it is obvious that if the access to and the exchange of data between databases becomes technically feasible, these technical means will be used, sooner or later. The choice for interoperability is therefore not a neutral one to be made on the mere basis of technical justifications. Furthermore, the EDPS objects to a more specific proposal in the communication — the use of biometrics as a primary key — since accuracy of biometrics is overestimated and such use would facilitate unwarranted interconnection of databases.

### Visa Information System

On 23 March 2005, the EDPS issued an opinion on the proposal for a regulation concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas. During 2006, he closely followed progress in Parliament and Council on this proposal.

In May 2006, the EDPS was consulted by the Presidency of the Council working party dealing with the proposal, on a number of modifications under consideration, in particular as to misuse of visa. In June 2006, the EDPS expressed appreciation for being consulted on this issue at this stage. However, he also expressed serious doubts whether the modifications were appropriate, both from a data protection point of view and in the context of the common visa policy.

### PNR issues

The judgment of the Court of Justice of 30 May 2006 in which the PNR agreement with the United States was annulled has had a big impact on the activities of the EDPS.

These were the first cases in which the EDPS used his powers to intervene. The EDPS supported the conclusions of the Parliament, that both the agreement with the United States and the decision by the Commission should be annulled. The Court decided to annul the decisions of the Council and the Commission on which the access of US authorities to passenger data (PNR data) of European airlines was based. The Court ruled that the wrong legal basis was chosen since the processing operations concern public security and activities of criminal law, and for that reason fall outside the scope of Directive 95/46/EC. To the Court, it is not decisive that the data had originally been collected for commercial purposes (the air transport of the passengers). The Court did not assess the arguments put forward by the EDPS and by others concerning the protection of fundamental rights.

Nevertheless, the EDPS considers this to be an important judgment in terms of data protection because it affects the scope of Directive 95/46/EC. The directive does not apply in situations where access to data is given by private companies for the purpose of law enforcement. This consequence of the judgment might create a loophole in the protection of Europeans.

The judgment required the conclusion of a new (interim) agreement with the United States, which was signed in October 2006 and which will expire by July 2007. The EDPS did not take part in the negotiations leading up to this interim agreement, nor did he formally advise on it, also since the objective of the negotiations from the European side was to reach an interim agreement with the same substance as the annulled one. The new agreement for the period after the expiration of the interim one will be of a fundamentally different nature. The preparations for this new agreement, closely followed by the EDPS have already started in 2006, inter alia by a Commission-proposal for a negotiations mandate <sup>(41)</sup>.

In addition, during 2006, the EDPS expressed his views on the exchange of passenger data with the

<sup>(41)</sup> This is not a public document.

United States in other ways. He issued a press release shortly after the judgment was announced. He also discussed the matter with the European institutions responsible for the negotiations and participated in discussions in the LIBE Committee of the European Parliament. Moreover, the EDPS actively participated on these issues in the framework of the Article 29 Working Party.

### Retention of traffic data

In July 2006, a new case was brought before the Court of Justice that could shed an additional light on the consequences of the PNR judgment, and in particular on the issue of the legal loophole. In the case C-301/06, *Ireland v. European Parliament and Council*, the validity of the data retention Directive 2006/24/EC<sup>(42)</sup> is at stake for reasons that there would be no legal basis under the third pillar to oblige private companies to collect and store communications data for the purpose of law enforcement.

In October 2006, the EDPS requested to the Court to intervene, in support of the conclusions of the defendants mainly because this case offers the possibility to clarify the Court judgment in the PNR cases. This position does not mean that the EDPS abandons his critical evaluation on the substance of the directive<sup>(43)</sup>.

### SWIFT

The issue of access of law enforcement authorities to databases created by private parties was also raised by the case of the secret transfers of European citizens' banking data to US authorities through the Society for Worldwide Interbank Financial Telecommunication (SWIFT). The EDPS conducted an inquiry and issued an opinion on the role of the European Central Bank in this case (see 2.5), and actively contributed to the opinion adopted by the Article 29 Working Party in November 2006.

<sup>(42)</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC.

<sup>(43)</sup> See his opinion of 26 September 2005 on the relevant Commission proposal.

### Public access to documents

In March 2006, the EDPS decided to intervene, in support of the conclusions of appellants, in three cases before the Court of First Instance on the relationship between public access to documents and data protection<sup>(44)</sup>. This offered an opportunity to elaborate on this subject in the light of the background paper on public access to documents and data protection published in July 2005<sup>(45)</sup>.

## 3.5. New developments

### 3.5.1. Technological developments

#### Enabling technologies for privacy and data protection

The European institutions invest continuously in research, implementation and use of new technologies in order to build a competitive European information society according to the Lisbon agenda. But the European information society will be sustainable only if these technologies are properly designed and implemented in such a way as to efficiently contribute to the European data protection framework and to a more secure environment.

The EDPS welcomed the Commission communication on 'A strategy for a secure information society'<sup>(46)</sup> published in 2006 and especially its following vision: 'a totally interconnected and networked everyday life promises significant opportunities. However, it will also create additional security and privacy-related risks'. 'Best available techniques' (BATs) which can efficiently contribute to data protection regulation and security requirements need therefore to be urgently identified. This selection, if frequently reviewed, will strengthen the symbiosis model of privacy and security requirements the European Union is developing.

<sup>(44)</sup> Cases T-170/03 (*British American Tobacco v. Commission*), T-161/04 (*Valero Jordan v. Commission*) and T-194/04 (*Bavarian Lager v. Commission*). A public hearing in the third case was held in September 2006, at which oral comments were made on behalf of the EDPS. In February 2007, the case had not yet been decided. See also paragraph 2.7 of this annual report.

<sup>(45)</sup> Available on the website: <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/pid/21>

<sup>(46)</sup> Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2006) 251, 'A strategy for a secure information society: dialogue, partnership and empowerment'.



Following new technological developments that may impact on data protection is part of the EDPS' mission.

In the preceding annual report, the EDPS identified new technological developments, such as RFID systems, biometrics and identity management systems, that are expected to have a major impact on data protection. The proper identification of privacy and security BATs for these developments will be decisive for their acceptance by the end user as well as for the European industry competitiveness.

The joint initiative in which the EDPS took part last November during the International Conference of Data Protection and Privacy Commissioners in London <sup>(47)</sup>, suggested drawing a parallel between the preservation of individual liberties and the preservation of the environment. 'Privacy and data protection may be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous.' Based on this parallel, surveillance can be compared with pollution and the expertise developed by the EU on the prevention and control of pollution <sup>(48)</sup> using the concept of BATs could offer

valuable lessons in order to mitigate the risks of a surveillance society.

### R & D for privacy and data protection

Privacy and data protection requirements need to be applied as soon as possible in the life cycle of new technology developments. The EDPS considers that the principle of 'privacy by design' should constitute an inherent part of the EU research and development efforts. At the end of 2006, the Commission announced and launched the seventh research framework programme <sup>(49)</sup> (FP7), the most important part of which will be devoted to information society technologies. In order to follow the FP7 closely, the EDPS decided first to take an active part to its launching event, the IST 2006 conference held in Helsinki, by having a stand in order to:

- identify at an early stage, the emerging trends which will drive this ambitious R & D effort;
- establish fruitful contacts with forthcoming research projects;
- raise awareness of the main stakeholders for the possible data protection aspects of their future research project;
- provide advice on the way to include data protection concerns in future proposals and research activities.

Based on this first experience, the EDPS will develop several models of contribution to targeted research projects of the FP7. Opinions on the methodologies implemented or on the results obtained could be envisaged. Research projects of the FP7 usually have the obligation to involve partners coming from several Members States. The EDPS could also, in this case, contribute to the cooperation between the corresponding data protection authorities which would be involved.

<sup>(47)</sup> See paragraph 4.5 and 5.1 of this annual report.

<sup>(48)</sup> <http://eippcb.jrc.es/>

<sup>(49)</sup> [http://cordis.europa.eu/fp7/home\\_en.html](http://cordis.europa.eu/fp7/home_en.html)

### 3.5.2. New developments in policy and legislation

The inventory 2007 gives an overview of the most important trends and risks related to data protection that are expected to affect the EDPS' consultative work and lists his priorities. It builds on the annual report 2005.

#### Area of freedom, security and justice

There have been rapid developments in the area of freedom, security and justice (in its wider sense, including Title VI of the EU Treaty). At the very end of 2006, the objectives of the German presidency of the Council were revealed and became even clearer in January 2007. The increased need for storage and exchange of personal data for law enforcement purposes, mentioned in the inventory 2007, plays an even more central role. For this reason, the presidency envisages tabling a formal proposal to transpose the Prüm Treaty into instruments of EU legislation.

This move would allow authorities of EU Member States to give one another automatic access to genetic records, fingerprints and traffic offences. It also implies obligations to store (and share) personal information such as DNA which fits within a second trend, the use of biometrics becoming more and more prevalent. Furthermore, a third continuing trend is the establishment and improvement of databases at a European level, supporting exchange between Member States, such as SIS II, VIS and the Europol information system. The fourth trend to mention is the increased pressure on the access and use of personal data for law enforcement purposes that had originally been collected for other purposes. A proposal has been announced to also open up for law enforcement the databases of Eurodac, established under the first pillar. Requests for this type of access also raise particular difficulties as a result of the pillar structure of the EU Treaty and the primacy of the protection provided for under the first pillar <sup>(50)</sup>.

For the EDPS, these trends require the establishment of an adequate framework for data protection in the third pillar, including the rules on effective division of responsibilities and on supervision of responsible entities. The unsatisfactory progress of the negotiations

on the Council framework decision will continue to require attention of the EDPS.

#### Other areas of specific attention

- Electronic communications and information society (Information Society and Media DG)

In the short term, the review of the EU regulatory framework (including Directive 2002/58/EC) will be an essential benchmark. In the long term, the trend seems to be a perspective of an information society where every person can be traced, for instance because of the growing importance of RFID.

- Public health (Health and Consumer Protection DG)

There is a general trend for increased collection and exchange of information related to health, which by nature (health data are sensitive data) presents risks for data subjects. This trend is even more important in the light of the growing digitisation of health data and in the light of the notion of traceability.

- Work-related issues (Employment, Social Affairs and Equal Opportunities DG).

The need for a special data protection regime at the workplace should be further examined and, separately, the exchange of social security in a closer cooperating EU.

- Anti-fraud (European Anti-Fraud Office, OLAF)

OLAF is of special importance to the EDPS, since it is a Community body under supervision of the EDPS with executive powers in the Member States. It exchanges data with law enforcement authorities of the Member States, authorities at EU level such as Europol and third countries and international organisations. This exchange requires safeguards, including on effective supervision.

- Transparency issues (Secretariat-General)

Initiatives aimed at modifying Regulation (EC) No 1049/2001 regarding public access to documents, which must clarify the relation between public access and data protection. The EDPS intends to issue an opinion and advise institutions where appropriate prior and after adoption of the relevant Commission proposals. The outcome of the pending cases before the Court of First Instance (see paragraph 3.4) may be relevant in this context.

<sup>(50)</sup> Article 47 of the EU Treaty.

**Consolidation and improvement**

The EDPS' working method will be consolidated and made effective in all EU policy areas. Energy and Transport DG will be the next service of the Commission with which the EDPS will establish cooperative contacts, as a result of legislative activities on computerised reservation systems for transport by air. The EDPS' ambition is to have good working relations with all services of the Commission by the end of 2007, as far as they could be relevant to his mission. The EDPS will build on internal communica-

tions within the Commission by the Commission's Secretary-General and the data protection officer that underline the competences of the EDPS. Specific aspects of Commission decisions (see also paragraph 3.2.1) will be given attention.

Relations with the Council and the European Parliament will also be intensified in order to enhance the effectiveness of the EDPS after the adoption of an opinion. The EDPS intends to build on existing good contacts and positive experience.



## 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<sup>(51)</sup>. Its tasks have been 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 uniform application of the directive, and in the interpretation of its general principles.

In April 2006, when adopting its work programme for 2006–07, the working party took an important decision<sup>(52)</sup>, with firm support of the EDPS. It decided to concentrate on a limited number of strategic issues aiming at contributing to a common understanding of key provisions of Directives 95/46/EC and 2002/28/EC and ensuring a better implementation of them.

In accordance with this programme, the working party has been addressing subjects which merit separate attention, such as the impact of radio frequency identification (RFID) and identity management, especially in e-government, and e-health patient records. At the same time, the working party developed a better common understanding of key concepts, such as ‘personal data’ and ‘consent’, and special rules for processing of medical data in Articles 2 and 8 of Directive 95/46/EC. The EDPS participated closely in these activities and looks forward to their results in the course of 2007.

In 2006, the EDPS also contributed to the working party’s activities in the field of international transfers to third countries. This concerned particularly the issue of airline passenger data, in the light of the European Court of Justice’s judgment in the PNR cases, and the subsequent need for negotiations with the United States (see paragraph 3.4). On this basis, the working party developed the outline of a long-term strategy and adopted various opinions<sup>(53)</sup> on related issues:

<sup>(51)</sup> 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.

<sup>(52)</sup> Work programme 2006–07, adopted on 5 April 2006 (WP 120). Accessible from: [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2006\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm)

<sup>(53)</sup> These and other working party opinions mentioned in the chapter are accessible from the same link as the work programme.

- Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of passenger name records to the United States, adopted on 14 June 2006 (WP 122);
- Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of passenger name records to the United States and the urgent need for a new agreement, adopted on 27 September 2006 (WP 124);
- Opinion 9/2006 on the implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data, adopted on 27 September 2006 (WP 127).

The working party issued a number of opinions on proposals for legislation. In some cases these proposals had been the subject of an opinion of the EDPS on the basis of Article 28(2) of Regulation (EC) No 45/2001. The EDPS opinion is a compulsory feature of the EU legislative process, but the opinions of the working party are of course also extremely useful, particularly since they may contain additional points of attention from a national perspective.

The EDPS therefore welcomes these opinions from the Article 29 Working Party, which have been quite consistent with opinions adopted by the EDPS. In another case, the EDPS preferred to collaborate even more closely in one single opinion, without issuing his own comments. Examples of good synergy between the working party and the EDPS in this field have been:

- Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, adopted on 25 March 2006 (WP 119) <sup>(54)</sup>;
- Opinion 6/2006 on the proposal for a Council regulation on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations, adopted on 9 August 2006 (WP 123) <sup>(55)</sup>;

<sup>(54)</sup> This opinion restated the essential safeguards for retention of traffic data, after adoption of Directive 2006/24/EC, for consideration at national level implementing the directive. See also EDPS opinion of 26 September 2005 on the Commission proposal.

<sup>(55)</sup> See also EDPS opinion issued on 15 May 2006.

- Opinion 8/2006 on the review of the regulatory framework for electronic communications and services, with focus on the e-privacy directive, adopted on 26 September 2006 (WP 126).

The EDPS also actively contributed to opinions highlighting the meaning of relevant provisions in the European data protection framework in different areas, such as:

- Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, adopted on 1 February 2006 (WP 117);
- Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006 (WP 118).

According to Article 46(f)(i) of Regulation (EC) No 45/2001, the EDPS must also cooperate 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 other assistance in the execution of their tasks. This cooperation takes place on a case-by-case basis. The SWIFT case was an example of multilateral cooperation in which the Article 29 Working Party <sup>(56)</sup> played a very useful role (see also paragraph 2.5).

The direct cooperation with national authorities is growing even more relevant in the context of international systems such as Eurodac and the proposed Visa Information System (VIS), which require effective joint supervision (see paragraph 2.9).

## 4.2. Council Working Party on Data Protection

The Austrian Presidency decided to convene two meetings of the Council Working Party on Data Protection. One of the objectives was to re-launch a discussion on its future role, keeping in mind that in the past this working party dealt with the foundations of the EC policy on data protection, such as Directive 95/46/EC, Directive 97/66/EC and Regulation EC (No) 45/2001. The Finnish Presidency supported this

<sup>(56)</sup> See Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), adopted on 22 November 2006 (WP 128).

initiative and convened a third meeting during the autumn of 2006.

The EDPS welcomed the initiative as a useful opportunity to ensure a more horizontal approach in first pillar matters. During the second meeting, he presented his annual report 2005. In the third meeting, the EDPS gave an overview of developments in his advisory role on proposals for new legislation.

The German presidency has decided to continue on the same basis with discussions on possible Commission initiatives and other relevant subjects in a first pillar context. The EDPS will be following these activities with great interest, and is available to advise and cooperate where appropriate.

### 4.3. Third pillar

Article 46(f)(ii) of Regulation EC (No) 45/2001 provides that the EDPS cooperates with the supervisory data protection bodies established under Title VI of the EU Treaty ('third pillar'), with a view to improving 'consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance'. These supervisory bodies are the Joint Supervisory Bodies (JSB) for Schengen, Europol, Eurojust and the Customs Information System (CIS). Most of these bodies are composed of (partly the same) representatives of national supervisory authorities. In practice, cooperation takes place with the relevant JSBs, supported by a joint data protection secretariat in the Council, and, more generally, with national DPAs.

The need for close cooperation between national DPAs and the EDPS has been made apparent in recent years by the steady increase of initiatives at European level to fight organised crime and terrorism, including different proposals for exchange of personal data.

In 2006, most attention centred around two relevant proposals under discussion in the Council. The first one was the Commission proposal for a framework decision on data protection in the third pillar, on which the EDPS issued an opinion on 19 December 2005. On 24 January 2006, the Conference of European Data Protection Authorities also adopted an opinion, which was consistent with the EDPS opinion. The second proposal was the Commission proposal for a framework decision on the exchange



Peter Hustinx during a press conference.

of information under the principle of availability, on which the EDPS issued an opinion on 28 February 2006 (see paragraph 3.3.3)<sup>(57)</sup>. Both proposals were interrelated, and this implied that the adoption of the first proposal was a precondition for the adoption of the second one.

At the Conference of European Data Protection Authorities held on 24 and 25 April 2006 in Budapest (see paragraph 4.4), a declaration was adopted. It reminds Member States that sharing personal information between their law enforcement authorities is permissible only on the basis of data protection rules ensuring a high and harmonised data protection standard at European level and in all participating States. Otherwise, the different levels of protection and the lack of common rules for access control to information could give rise to situations where minimum data protection standards are not respected. As the confer-

<sup>(57)</sup> See: 'A framework in development: third pillar and data protection', in: *Ochrona danych osobowych wczoraj, dziś, jutro / Personal data protection yesterday, today, tomorrow*, Warsaw 2006, pp. 132–137 (in English) and p. 137–142 (in Polish). Also available at the EDPS website (on 12 May): <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/23>

ence had already pointed in 2005, the existing legal instruments applicable in the EU on data protection were too general to provide effective data protection in the field of law enforcement.

Therefore, the conference welcomed the proposal of the Commission to harmonise and strengthen data protection for activities of police and judicial authorities through the establishment of data protection safeguards for the third pillar, that are to be applied when exchanging information under the principle of availability. It also stressed that there is no alternative to creating a high and harmonised data protection standard in the EU third pillar. This is a consequence of the Hague programme, according to which the safeguarding of freedom, security and justice are indivisible elements of the European Union as a whole <sup>(58)</sup>.

However, it appeared that this approach was not shared by all Member States <sup>(59)</sup>. As a result, the progress in Council on the required data protection framework for the third pillar has been unsatisfactory, in spite of the efforts of consecutive presidencies. At the same time, initiatives to promote and facilitate exchange of information have progressed well <sup>(60)</sup>. On 29 November 2006, the EDPS issued a second opinion on the data protection framework, warning the Council not to lower EU citizens' rights in third pillar data protection (see paragraph 3.3).

In Budapest, it was also decided to entrust the Police Working Party, supported by the Data Protection Secretariat, with the task of studying a number of issues and to report to the next spring conference. This involved different issues relating to the scope and implications of the principle of availability, as well as the need for additional safeguards. It also required the development of proposals to further harmonise the practice in the different Member States concerning the right of access.

<sup>(58)</sup> This message was repeated in a statement of the European data protection authorities adopted in London on 2 November 2006. Both statements are available at EDPS website: <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51>

<sup>(59)</sup> See also: House of Lords, European Union Committee, 'Behind closed doors: the meeting of the G6 interior ministers at Heiligendamm', report with evidence, July 2006, inter alia containing statements of the EDPS (oral evidence on 7 June 2006).

<sup>(60)</sup> See Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, p. 89. See also initiatives of the German presidency to transpose the Prüm Treaty into the legal framework of the EU, which will be analysed by the EDPS in 2007.

## Schengen and Europol

The cooperation of the EDPS with the JSA Schengen resulted in January 2006 in a model for 'coordinated' supervision of SIS II. This model has now been laid down in Articles 44 to 46 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) <sup>(61)</sup>.

On 26 June 2006, the JSB Europol issued an opinion with respect to the proposal for a Council decision concerning access for consultation of the Visa Information System (VIS) by authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist and other serious criminal offences. This opinion highlights a number of points, which were also raised in the EDPS opinion of 20 January 2006 (see paragraph 3.3.3), but focuses more on the position of Europol.

The EDPS also benefited from a close cooperation with the JSB Europol and the Data Protection Secretariat in the analysis of a draft proposal for a Council decision establishing the European Police Office (Europol), adopted by the Commission in December 2006. This proposal aims to provide Europol with a new and more flexible legal basis in EU law and to replace the existing Europol Convention. On 16 February 2007, the EDPS delivered an opinion on this proposal.

## 4.4. European conference

Data protection authorities from Member States of the EU and the Council of Europe meet annually for a spring conference to discuss matters of common interest and to exchange information and experiences on different topics. The EDPS and the Assistant Supervisor took part in the conference in Budapest on 24 and 25 April 2006 which was hosted by the Hungarian Commissioner for Data Protection and Freedom of Information. This conference coincided with the 10th anniversary of the Hungarian DPA <sup>(62)</sup>.

<sup>(61)</sup> See also paragraph 3.4 of this annual report.

<sup>(62)</sup> See: 'Adequate protection' — Opinion 6/99 of the Article 29 Working Party revisited, published in: *Tízéves az Adatvédelmi Biztos Irodájára / Ten years of the DP and FOI Commissioner's Office*, Budapest 2006, pp. 79–87 (in Hungarian) and pp. 251–259 (in English). Also available at EDPS website (on 27 April 2006): <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/26>

Mr András Baka, Hungarian judge at the European Court of Human Rights, made introductory remarks about the Court's case-law on data protection and freedom of information.

The EDPS specifically contributed to the session focusing on 'Data protection in the third pillar'. The Assistant Supervisor spoke at the session on 'Whistle-blowing and integrity lines', drawing from experience in EU institutions and OLAF in particular. Other subjects dealt with at the conference were: 'RFID and geo-localisation', 'Historical and scientific research', 'National health databases', 'Genetic data', and 'Effectiveness of Commissioners'. The conference also adopted a number of important documents (see paragraph 4.4).

The next European conference will be held in Larnaka (Cyprus) on 10 and 11 May 2007, and will take stock of relevant issues requiring attention.

#### 4.5. International conference

Data protection authorities and privacy commissioners from Europe and other parts of the world, including Canada, Latin America, Australia, New Zealand, Hong Kong, Japan and other jurisdictions in the Asia-Pacific region, have met annually for a conference in the autumn for many years. The 28th International Conference of Data Protection and Privacy Commissioners took place in London on 2 and 3 November 2006 and was attended by delegates from 58 countries around the world.

This conference was unusual in that it was entirely devoted to one single theme of major importance: 'The surveillance society'. The UK Information Commissioner had also commissioned a background report on the subject, prepared by a group of UK researchers cooperating in the 'surveillance studies network' <sup>(63)</sup>. The first day of the conference consisted of presentations from different perspectives, and the second day was devoted to analysis and discussion among participants, including a closed session for Commissioners to draw conclusions.

A number of themes were emphasised by Commissioners in the closing communiqué:

- *The 'surveillance society' is already with us.* Surveillance involves the purposeful, routine and systematic recording by technology of individuals' movements and activities in public and private spaces. There are already many examples of this in everyday life.
- *Surveillance activities can be well-intentioned and bring benefits.* So far the expansion of these activities has developed in relatively benign and piecemeal ways in democratic societies — not because governments or businesses necessarily wish to intrude into the lives of individuals in an unwarranted way.
- *But unseen, uncontrolled or excessive surveillance activities also pose risks that go much further than just affecting privacy.* They can foster a climate of suspicion and undermine trust. The collection and use of vast amounts of personal information by public and private organisations leads to decisions which directly influence peoples' lives.
- *Privacy and data protection regulation is an important safeguard but not the sole answer.* The effects of surveillance on individuals do not just reduce their privacy. They also can affect their opportunities, life chances and lifestyle. Excessive surveillance also impacts on the very nature of society.
- *A systematic use of impact assessments should be adopted.* Such assessments would include but be wider than privacy impact assessments, identifying social impact and opportunities for minimising undesirable consequences for individuals and society.
- *The issues are wide ranging and cannot be taken forward by data protection or privacy regulators alone.* Engagement should be a common cause for all who are concerned about these developments. Commissioners should work alongside civil society organisations and governments, private sector, elected representatives and individuals themselves to guard against unwarranted consequences.
- *Public trust and confidence is paramount.* Although much of the infrastructure of the surveillance society has been assembled for benign purposes, continued public trust cannot be taken for granted. Individuals must feel confident that any intrusion

<sup>(63)</sup> See documents available at EDPS website: <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51>

into their lives is for necessary and proportionate purposes.

The EDPS is committed to bringing this process forward. This was the background for his cooperation in the 'London Initiative' — 'Communicating data protection and making it more effective' — discussed in paragraph 5.1.

The next international conference will be held in Montreal from 26 to 28 September 2007 under the title 'Privacy horizons: terra incognita'.

## 5. Communication

### 5.1. Introduction

Privacy and personal data protection are about people. The perception of what these rights constitute may differ from one person to another as the notions are intrinsically linked to the type of society we live in — each with its own history and culture — and to everyone's personal experience in life. Yet, everyone has the same fundamental rights and these rights impose certain conditions <sup>(64)</sup> that political representatives and policymakers are obliged to respect when adopting or proposing new measures that have an impact on private life, or on the way in which personal data are collected and used. It is thus of vital importance that policymakers are aware of the implications and their margins of manoeuvre.

Legal rules on privacy and protection of personal data also provide for specific rights and obligations at a more practical level. Data subjects' rights of access and correction of data, or the rights to object or withhold consent to the processing of personal data, are also relevant for EU institutions and bodies. So are obligations to ensure that personal data are only processed for legitimate purposes and on lawful grounds, that adequate transparency is provided to data subjects and that sufficient security measures apply. It is therefore also of vital importance that all parties involved are aware of their rights and obligations, as well of the practical relevance of these rights and obligations in various situations which are important for them. Protection of privacy and personal data can only be made a reality if the relevant rules are complied with in practice.

<sup>(64)</sup> See, for example, Article 8 of the European Convention on Human Rights, Articles 7 to 8 of EU Charter of Fundamental Rights, Directive 95/46/EC and Regulation (EC) No 45/2001. See also ECJ decision of 20 May 2003 in joined cases C-465/00, C-138/01 and 139/01 (*Österreichischer Rundfunk*).

Research suggests that Europeans continue to care about the privacy and security of their personal information <sup>(65)</sup>. This is highly relevant in a society which is becoming more dependent on the use of information and communication technologies. In many fields of life, at home, at work, when shopping, using a mobile phone or surfing on the web, most people collect and share information, and leave a wealth of personal traces behind. Yet, many find it difficult to see how this relates, in practical terms, to the need for continued protection of their privacy and personal information, and most of all, what this means for their own daily life. This is where communication plays a crucial role, as a powerful means of raising awareness and informing individuals on how to deal with this reality in a responsible way and make the best possible use of their rights. This is, in short, often referred to as 'empowerment'.

At the 28th International Conference <sup>(66)</sup> of Data Protection and Privacy Commissioners in London, a statement <sup>(67)</sup> 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, the UK Information Commissioner and the EDPS (now also referred to as 'London Initiative'). As one of the architects of the initiative, the EDPS will actively contribute to the follow-up together with national data protection authorities, and share available experience and best practice.

<sup>(65)</sup> See, for example, Special Eurobarometer 2003 and UK Information Commissioner's annual track research 2004–06.

<sup>(66)</sup> See also paragraph 4.5 of this annual report.

<sup>(67)</sup> Available at EDPS website: <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51>

Some of the main points in the London Initiative are:

- *Protection of citizens' privacy and personal data is vital* for any democratic society, on the same level as freedom of the press or freedom of movement. Privacy and data protection may, in fact, be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous.
- *Commissioners should develop a new communication strategy* in order to make the public and relevant stakeholders more aware of these rights and their importance. Commissioners should initiate powerful and long-term awareness-raising campaigns and measure the effects of these actions.
- *Commissioners should also communicate better* about their own activities and make data protection more concrete. Only when these activities are meaningful, accessible and relevant for the public at large, is it possible to gain the necessary power to influence public opinion and to be heard by decision-makers.
- *Commissioners should assess their efficiency and effectiveness*, and, where necessary, adapt their practices. They should be granted sufficient powers and resources, but should also use them in a selective and pragmatic manner, while concentrating on serious and likely harms, or the main risks facing individuals.
- *Commissioners should reinforce their capacities in technological areas*, with a view to advanced studies, expert opinions and interventions, in close interaction with research and industry in the field of new technology, and share this work together. The excessive 'legal' image of data protection must be corrected.

>>>

<<<

- *Commissioners should promote the involvement of other stakeholders* of data protection and privacy, at national or international level, such as civil society and NGOs, to develop strategic partnerships where appropriate, with a view to making their work more effective.

Commissioners will undertake a programme of follow-up activities along these lines and will consider and evaluate progress made at their next international conference.

## 5.2. Main activities and target groups

During 2006, communication work at EU level continued to centre on the three main activities — supervision, consultation and cooperation — each with specific target groups. As the EDPS and the Assistant Supervisor had been in office for more than two years, less effort was made on raising awareness about the authority among the other institutions than in previous years. Instead, focus lay on specific issues dealt with.

### Supervision

In relation to the task to ensure that the EC institutions and bodies respect their data protection obligations, the following two target groups have been identified.

- The individual: data subjects in general, and staff of the EC institutions and bodies in particular. This relates to the 'rights perspective' <sup>(68)</sup> with a focus on empowering the data subject, by making sure that they are properly informed of processing operations concerning them, as well as of their rights of access, rectification, blocking, etc.
- The institutional system: focusing on the obligations <sup>(69)</sup> for those who have an administrative responsibility for the processing operations. In the EC institutions and bodies, these are the con-

<sup>(68)</sup> See Articles 13-19 of Regulation (EC) No 45/2001 (rights of data subjects).

<sup>(69)</sup> See Articles 4-12 of Regulation (EC) No 45/2001 (rules on lawful processing, information to data subject).

trollers and the Data Protection Officers (DPO). Because of its size, the European Commission has also introduced an additional layer — the data protection coordinator (DPC) — which has a delegated responsibility in the directorates-general of the Commission.

In terms of the ‘rights perspective’, there have been a number of more general efforts in addition to the obligation of the controller to inform the data subjects of any given processing operation. Examples include an interview and other contributions to the weekly internal newspaper of the Commission, which has a print run of more than 50 000 copies and which is also distributed to staff in other institutions.

In terms of the ‘obligations perspective’, communication focused primarily on regular meetings with the network of DPOs. However, there were also meetings with various other key actors, such as when the EDPS met with the secretary-general and the directors-general of the Commission to discuss progress in implementation of data protection measures.

### Consultation

In relation to the task to promote good data protection in new legislation and new policies, the target group can be referred to as ‘EU political stakeholders’. The EDPS advice in the first stage is thus directed at the Commission, and in the second at the European Parliament and the Council. When an opinion has been sent to the different stakeholders and is published on his website, the EDPS usually presents his views in the relevant committee (such as LIBE) of the European Parliament or the relevant working party or steering committee (such as Article 36 Committee) of the Council.

Legislative opinions are, in general, made public together with a press release which is sent to some 100 regular media contacts. This often results in media coverage, as do participation in those committee meetings that are public, and therefore are often attended by journalists. Most of the requests for interviews (see paragraph 5.6) relate to the consultative role, and granting such requests is another way of promoting the EDPS’ opinions.

### Cooperation

Working together with ‘data protection colleagues’ throughout Europe and further afield has the aim of

promoting a consistent level of data protection. This relates to information systems where the EDPS exercises a part of the supervisory role, such as for Eurodac. However, it also deals with sharing experience and best practice on case handling, either bilaterally or collectively, with other data protection authorities.

Communication in these situations is often integrated in other activities or undertaken jointly with the other actors involved. Examples are the cooperative work within the Article 29 Working Party, or within the International Conference of Data Protection and Privacy Commissioners, where the organisers in London took a successful lead vis-à-vis media.

## 5.3. Website

The website is the EDPS’ most important communication tool. Its first version was created during the first half of 2004 and its basic structure was fairly simple. New sections and new types of documents were added, while the number of downloadable documents increased significantly. By autumn 2005, it was felt that its natural limits were in sight. Therefore, a project to create a second generation website was initiated and this work went on throughout 2006. A completely new structure, built around the three main tasks, and a new visual identity were elaborated. A subcontractor was involved with the preparatory studies and the production, in close cooperation with the European Parliament. The second generation website went online in February 2007 with some delay on the original planning. Further functionalities will be developed during 2007.

The average number of visits continued to increase during 2006 from 1 000 to 1 500 visits per week. Website traffic increased when many new documents were uploaded on to the website. When press releases were issued, this also resulted in more visits. The rather low ‘surfing tendency’, with Internet users visiting around three pages per visit, is expected to change rapidly due to the launching of the new website. The number of visits is also expected to increase.

A welcome page in all present Community languages will show visitors to documents that are available in their own language. Most information is now available in at least English and French. The intention is to provide German as a third language in the near future.



Peter Hustinx and Joaquín Bayo Delgado presenting their Annual Report for 2005 during a press conference.

## 5.4. Speeches

The EDPS continued to invest considerable time and effort in explaining his mission and raising awareness about 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. He also gave a number of interviews to relevant media.

The EDPS frequently appeared in the European Parliament's LIBE Committee or at related events. On 24 January, he presented his opinion on a proposal for access to the Visa Information System (VIS) for internal security and law enforcement purposes. On 21 February, he met with MEPs on other aspects of the VIS. The same day, he also presented his opinion on a proposal for a framework decision on data protection in the third pillar. On 27 April, he presented his annual report for 2005. On 30 May, he made a contribution to a seminar on interoperability of databases. In a joint meeting of LIBE and representatives of national parliaments on 22 June, he presented his views on the transfer of airline passenger data (PNR) to the United States. On 4 October, he spoke at a public hearing on the SWIFT case. On 19 October, he made a contribution to a public seminar of ALDE on security and freedom. On 18 December, he delivered a speech at a public seminar on police cooperation in the EU.

Contacts with other parliamentary committees and services are also developing. On 26 June, the EDPS

delivered a speech at a seminar of the EP Legal Service. Moreover, on 23 November, he spoke at a public hearing on social security before the EMPL Committee. On 22 December, he presented his opinion on a revision of the financial regulation and its implementing rules before the Cocobu Committee.

On 12 January, the EDPS presented his opinion on data protection in the third pillar at a meeting of the relevant working party of the Council. On 19 May and 27 October, he contributed to discussions in the Council working party on data protection, which is to deal with various first pillar issues.

Other EU institutions and bodies were of course also on the list. On 3 April, the EDPS gave a speech for the director-general and management of OLAF on the need for implementation of adequate data protection measures in their activities. On 17 May, he spoke at a public seminar on RFID at the European Commission. On 18 May, he delivered a speech at the European Investment Bank. On 29 June, he presented at a weekly meeting of the secretary-general and the directors-general of the Commission. On 5 December, he spoke at a bureau meeting of the Committee of the Regions.

In the course of the year, the EDPS also visited a number of Member States. On 29 March, he gave a speech at the first European Data Protection Conference for public and private sector representatives in Madrid. On 24 April, he spoke at the Spring Conference of

European Data Protection Commissioners in Budapest. On 11 May, he presented at a conference on Data Protection and Public Security in Warsaw. On 23 May, he delivered a speech on 'Data protection and transparency in the EU institutions' at the Fourth International Conference of Information Commissioners in Manchester. On 1 June, the EDPS was at a conference of the International Federation of Computer Law Associations in Amsterdam for a speech on recent developments in data protection. On 7 June, he testified before a subcommittee of the House of Lords in London on different issues relating to data protection in the third pillar. On 27 June, he addressed the International Banking Forum on Financial Crime in Brussels.

On 27 September, the EDPS delivered a speech at the Fifth Annual Data Protection Compliance Conference in London. On 28 September, he spoke at a seminar of the Finnish Presidency on the European Information Society near Helsinki. On 4 October, he gave a speech at the first International Conference on Data Protection in Plurinational and Federal States in Barcelona. On 8 November, he delivered a speech at a workshop of the International Pharmaceutical Privacy Consortium in Frankfurt. On 9 November, he spoke about the 'European institutional framework for data protection' at the Academy for European Law in Trier. On 14 November, he delivered a speech on data retention at the ARMA Round Table in Brussels. On 15 December, he gave a speech on his positions on biometrics at a meeting with the Dutch Biometrics Forum in Brussels.

The Assistant Supervisor made similar presentations in Budapest, Warsaw, Madrid and Barcelona, *inter alia* for the Spanish Judicial School, on data protection in the third pillar.

## 5.5. Newsletter

Five issues of the newsletter were published in 2006. The number of subscribers rose steadily, from some 250 people in January to around 460 by the end of the year. Among others, members of the European Parliament, EU staff and staff of national data protection authorities make use of the newsletter to follow the most recent activities of the EDPS. The newsletter provides opinions on legislative proposals and opinions on prior checks, with relevant background

and context, together with other recent developments. An automatic subscription feature is available on the website <sup>(70)</sup>.

The newsletter is an efficient tool to draw attention to recent additions to the website and allows them to be circulated widely. This increases visibility of the website and encourages subsequent visits. The network community interested in data protection activities at EU level is thus growing both in size and intensity, at least in number of interactions.

## 5.6. Press service

The press service is in charge of contacts with journalists, writing press releases and organising press conferences. The press officer also leads a flexible information team which is involved in any promotional activities (EU Open Day, etc.), as well as in producing information material aimed at the public and to journalists.

Two press conferences were organised in 2006. In mid-April, the annual report 2005 was presented and the main message was 'consolidating the EDPS'. The press conference highlighted the difference between 2004 when the authority was set up, and its second year of business. As the year continued, there was a growing impression of a widespread misconception that protection of privacy and personal data unduly holds back the fight against terrorism and organised crime. Therefore, marking the mid-term of their five-year mandates, the EDPS and the Assistant Supervisor held a second press conference in mid-September, focusing on the right to privacy in the EU and its legitimate and essential role in policymaking.

These well-attended press conferences covered both what the EDPS does in terms of ensuring that the Community institutions and bodies comply with their data protection obligations and in terms of advice on new legislation and new policies. In addition, more than 20 interviews were organised throughout the year, with printed as well as with audiovisual media. The majority of the requests for interviews came from 'EU Press' — media covering EU affairs for a target group which works with EU affairs. However, interviews were also given to more national media with a view to reaching out further than the Brussels envi-

<sup>(70)</sup> <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/27>



Peter Hustinx being interviewed by a journalist.

ronment, and to be also somewhat present in discussions in the Member States. Three such examples are interviews with German and Swedish Radio and with a Slovenian daily.

Requests for interviews which concerned matters falling outside the institutional role of the EDPS have been declined. Such requests come to the press service on at least a weekly basis, and they often lead to background information and the contact details of the responsible authority being passed on.

## 5.7. Information or advice

The number of requests for information and requests for advice rose by some 70 % during 2006. More than 170 requests came from students and other interested citizens, as well as from project managers and lawyers, spanning a wide range of topics.

More than 80 % of the requests were classified as 'for information' — a broad category which comprises general questions on EU policies, but also questions relating to data protection in the Member States as well as in the EU administration. Examples are questions about spam e-mails and identity fraud, on privacy and Internet, as well as on how to comply with Directive 95/46/EC when projects involve activities in several Member States.

Requests of a more complicated nature which require more analysis are classified as 'for advice'. These

account for close to 20 % of the requests. Two such examples relating to how to deal with public access to documents containing personal data are: what information to make available on lobbyists accredited to the European Parliament <sup>(1)</sup>, and whether photos of staff taken for security badges could be put on the 'who's who' of an institution.

Just as in 2005, the bulk of the requests were received in English and French, which allowed for fast replies, virtually always well within 15 working days. However, a sizeable number of requests also came in other official languages, some of which required the help of the translation service, and which therefore took longer to deal with. These requests are also used to develop new content for the website, so as to inform visitors and prevent unnecessary queries or complaints, as much as possible.

## 5.8. EU Open Day

The 2006 Open Day took place on 6 May. All the main EU institutions and bodies participate in the event which becomes something of a street festival which animates the EU headquarters area in Brussels, between the central buildings of the European Parliament and the Commission.

<sup>(1)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/06-08-31\\_transparency\\_lobbyists\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/06-08-31_transparency_lobbyists_EN.pdf)



EDPS staff manning the stand inside the European Parliament during the Open Day on 6 May 2006.

A stand and some smaller promotional material (pens, post-its and USB-sticks) were developed for use during the Open Day as well as for other occasions. The EDPS stand was put up inside the European Parliament and more than 200 people took part in a quiz on data protection issues, which inspired discussions about privacy and data protection in Europe.



## 6. Administration, budget and staff

### 6.1. Introduction: developing the new institution

The development of the EDPS as a new institution <sup>(72)</sup> continued on the basis established in 2005, with the aim of further consolidating its positive start. In 2006, the EDPS gained additional resources both in terms of his budget (increasing from EUR 2 879 305 to EUR 4 138 378) and his staff (from 19 to 24).

The administrative environment is gradually being extended on the basis of annual priorities, taking account of the needs and size of the institution. The EDPS has adopted various internal rules <sup>(73)</sup> necessary for the proper functioning of the institution. A staff committee has been created. It is closely associated to general implementing provisions for the Staff Regulations and to other internal rules adopted by the institution. A report on the implementation of internal control standards was prepared by the EDPS services. The first internal audit was organised by the internal auditor and the conclusions will be delivered in 2007.

Collaboration with other institutions — the European Parliament, the Council and the European Commission — was further improved, allowing for considerable economies of scale. A three-year extension of the administrative cooperation agreement of 24 June 2004 was signed in December. Slower performance of some tasks, connected to the principle of shared assistance (mainly related to the access to administrative and financial software) was still noted, but this should be

resolved in 2007. The EDPS took over some of the tasks which were originally performed by other institutions.

The premises originally made available to the EDPS have been enlarged and the EDPS now occupies two floors in the European Parliament's building, Montoyer 63.

### 6.2. Budget

A budget estimate for the year 2006 was drawn up in March 2005. This was the first estimate that the EDPS carried out without relying on the support of the European Parliament's services (as in 2004 and 2005).

The budget adopted by the budgetary authority for 2006 was EUR 3 583 833. This represents a 24.5 % increase compared with the 2005 budget. An amended budget of EUR 4 138 378 was adopted on 27 September 2006 as a consequence of a considerable increase of the Supervisor's opinions on proposals for legislation, which have to be published in the Official Journal, and the impact of these publications on the number of translations required.

The EDPS decided to apply the Commission's internal rules for the implementation of the budget to the extent that those rules are applicable to the structure and scale of the organisation and where specific rules have not been laid down.

Assistance from the Commission continued, particularly regarding the accounts, since the Accounting Officer of the Commission was also appointed as the Accounting Officer of the EDPS.

<sup>(72)</sup> Article 1b of the Staff Regulations of officials of the European Communities and Article 1 of the Financial Regulation provide that, for the purposes of these regulations, the EDPS shall be treated as an institution of the Communities. See also Article 43.6 of Regulation (EC) No 45/2001.

<sup>(73)</sup> A list of administrative agreements and decisions is available in Annex I.



Parts of the human resources team discussing a dossier.

In its report on the financial year 2005, the Court of Auditors stated that the audit had not given rise to any observations.

### 6.3. Human resources

The EDPS benefits from the very effective assistance of the Commission's services, regarding tasks relating to the personnel management of the institution (including two appointed members and 24 staff).

#### 6.3.1. Recruitment

As a recently created institution, the EDPS is still in a building phase, and will remain so for some years to come. The growing visibility is having the effect of an increase in workload, together with an expansion of tasks. The significant growth of the workload in 2006 has been described in previous chapters. Naturally, human resources have a fundamental role to play in this context.

Nevertheless, the EDPS has chosen initially to restrict expanding in tasks and staff, using controlled growth

to ensure that new staff were fully taken on board and adequately integrated and trained. For that reason, the EDPS called for the creation of just five posts in 2006 (three AD <sup>(74)</sup>, two AST <sup>(75)</sup>). This request was authorised by the budgetary authority, with the number of staff increasing from 19 in 2005 to 24 in 2006. At the beginning of the year, vacancy notices were published, and all the posts were filled in the course of the year.

The Commission's assistance in this area has been valuable, particularly the assistance of the Paymaster's Office (PMO) and of the Medical Service. In 2006, the EDPS has also developed social activities. The excellent working relationship with other institutions, in particular with the Council, the Committee of the Regions, the European Parliament and the Ombudsman allowed for exchange of information and best practice in this area.

The EDPS has access to the services provided by EPSO and participates in the work of its Management Board, presently as an observer.

<sup>(74)</sup> Administrators.

<sup>(75)</sup> Assistants.

### 6.3.2. Traineeship programme

The traineeship programme was created in 2005. The main objective is to offer recent university graduates the opportunity to put their academic knowledge into practice, thereby acquiring practical experience of the day-to-day activities of the EDPS. As a result, the EDPS increases his visibility to younger EU citizens, particularly those university students and young graduates who have specialised in data protection.

The main programme hosts between two and three trainees per session, with two five-month sessions per year. In 2006, the programme hosted two trainees per session, the majority specialised in the field of data protection. The first session started in October 2005 and finished in the end of February 2006. The results of that session were extremely positive. The trainees contributed both in theoretical and practical work, at the same time gaining first-hand experience.

In addition to the main traineeship programme, special provisions have been established to accept university students and PhD students for short-term, non-remunerated traineeships. This second part of the programme gives young students an opportunity to conduct research for their thesis, under specific limited admission criteria. This is done in accordance with the Bologna process and an obligation for university students to complete a traineeship as part of their studies. At the beginning of the year, one PhD student was selected for a two-month, non-remunerated traineeship. These non-remunerated traineeships are limited to exceptional situations and subject to specific admission criteria.

In addition to the trainees specialised in data protection, one candidate with background in business and finance was selected for a traineeship from October 2006 to February 2007 in the Human Resources, Administration and Budget Unit.

The EDPS has benefited from administrative assistance of the Commission's Education and Culture DG Traineeship Office, which has continued to provide valuable support thanks to the extensive experience of its staff, on the basis of a service-level agreement signed in 2005. At the same time, cooperation with the traineeship offices of other European institutions continued, in particular with the Council, the Committee of the Regions and the European Economic and Social Committee.

### 6.3.3. Programme for seconded national experts

The programme for seconded national experts (SNE) was launched in January 2006, following the creation of its legal and organisational basis in autumn 2005 <sup>(76)</sup>.

The secondment of national experts enables the EDPS to benefit from the professional skills and experiences of staff from data protection authorities (DPAs) in the Member States. This programme also enables national experts to familiarise themselves with data protection in the EU setting (in terms of supervision, consultation and cooperation). At the same time the EDPS increases his visibility in the field at operational level.

In order to recruit national experts, the EDPS directly addresses the national DPAs. National permanent representations are also informed of the programme and invited to assist in seeking suitable candidates. The Commission's Personnel and Administration DG provides valuable administrative assistance for the organisation of the programme.

The programme started with the secondment of one expert from the Hungarian DPA — the Commissioner for Data Protection and Freedom of Information — as from mid-January 2006.

### 6.3.4. Organisation chart

The EDPS' organisation chart has remained the same since 2004: one unit, now with seven people, is responsible for administration, staff and the budget; the rest of the 17 staff deal with operational data protection tasks. They work under the direct authority of the Supervisor and the Assistant Supervisor in two fields, mainly dealing with supervision and consultation. Some flexibility has been maintained in allocating tasks to staff, since the activities of the office are still evolving.

### 6.3.5. Training

EDPS staff has access to general as well as language training courses organised by other institutions, mainly by the Commission, and to the courses run by the European Administrative School (EAS).

<sup>(76)</sup> EDPS decision of 10 November 2005.

As to the language training, most cooperation is organised via the Interinstitutional Committee for Language Training, to which the EDPS participates as a member. In 2006, the member institutions signed an agreement on the harmonisation of the cost of the interinstitutional language courses.

Access to the training courses organised by the EAS has been assured by the service-level agreement signed with the School in 2005.

During 2006, the EDPS launched a proposal aimed at the development of a training policy based on the specific activities of the institutions as well as on its strategic objectives. The objective is to become a centre of excellence in the field of data protection, improving staff knowledge and skills so that EDPS values are fully integrated among staff.

The cooperation with the European Administration School allowed the EDPS to organise a first team-building exercise with a view to achieving common goals and developing a clear and unique identity.

## 6.4. Administrative assistance and interinstitutional cooperation

### 6.4.1. Extension of the administrative cooperation agreement

A significant step in 2006 was the three-year extension of the interinstitutional cooperation agreement concluded in June 2004 with the Secretaries-General of the Parliament, the Council and the Commission. This cooperation is of considerable value to the EDPS, since it gives access to expertise within the other institutions in the areas where assistance is provided and since it allows for economies of scale.

On the basis of this agreement, cooperation continued with various Commission services <sup>(77)</sup>, with different European Parliament's services (IT services, particularly with arrangements for the second generation of the website; fitting out of the premises, building security, printing, mail, telephone, supplies, etc.) and with the Council (translations).

---

<sup>(77)</sup> Personnel and Administration DG, Budget DG, Internal Audit Service, Justice, Freedom and Security DG, Education and Culture DG, Employment, Social Affairs and Equal Opportunities DG and the Paymaster's Office.

To facilitate cooperation between Commission departments and the EDPS, direct access from EDPS premises to the Commission's main human resources and financial management software was requested in 2005. Such direct access, which would improve the exchange of information and make it possible for files to be managed more effectively and rapidly by both the EDPS and the Commission's services, has unfortunately only been possible for SI2 and partially for Syslog, but not yet for the other software (e.g. ABAC) <sup>(78)</sup>. EDPS envisages intensifying cooperation in this field and hopes that the access will be completed during 2007.

The implementation of the service-level agreements signed in 2005 with the various institutions and their departments has been assured. These include:

- the agreement with the Council, which provides the EDPS with assistance in translation; this assistance is fundamental as the number of documents to translate grew considerably;
- the agreement with the Commission's Traineeships Office (within Education and Culture DG) which enabled the continuation of the traineeship programme in 2006;
- the agreement with the Commission's Employment, Social Affairs and Equal Opportunities DG provided the EDPS with the necessary technical assistance to create a portable stand, the elaboration of a logo and a new styling of the website.

### 6.4.2. Follow-up of interinstitutional cooperation

Interinstitutional cooperation is fundamental for the EDPS and for the further development of the institution. During 2006, in addition to the administrative agreement, interinstitutional cooperation has become an everyday reality allowing an increase of the efficiency in many areas of administration.

Participation in the interinstitutional call for tenders for furniture continued, allowing the institution to progress towards some autonomy as regards fitting-out of office space.

The development of a new website became possible thanks to cooperation with different services of the European Parliament which gave the EDPS the opportunity to use their framework contracts. On the basis

---

<sup>(78)</sup> Syslog is an information system for electronic management of training courses. SI2 and ABAC are systems for accounting management.

of the Parliament's advice, the EDPS signed an agreement with a consultant included in their framework contract for a total remake. The second generation website was launched in January 2007.

In 2006, the EDPS signed an administrative assistance agreement with the European Network and Information Security Agency (ENISA), defining the implementing arrangements for the security audit of the Eurodac database, as well as the conditions for the conduct of this cooperation (see paragraph 2.9).

The EDPS continued to participate in various inter-institutional committees; however, because of the size of the institution, such participation had to be limited to just a few committees. This participation contributed to increase the visibility of the EDPS in the other institutions and encouraged the continuous exchange of information and good practice.

#### 6.4.3. External relations

The process of having the institution recognised by the Belgian authorities was completed, enabling the EDPS and his staff to have access to the privileges and immunities laid down in the Protocol on the Privileges and Immunities of the European Communities.

### 6.5. Infrastructure

With the increased number of staff, the EDPS was experiencing office space problems. This was resolved by acquiring additional space in 2006, the seventh floor of the European Parliament building Montoyer 63, and the EDPS can now use two consecutive floors in the building. Considering the sensitivity of the data that the EDPS processes, the new floor was secured with the same protection system as the sixth floor, in order to limit access only to authorised persons.

Regarding furniture, the administrative assistance from the European Parliament ended in 2005. The EDPS therefore started working independently on this matter, taking part in an interinstitutional tender.

On the basis of an administrative cooperation agreement, the European Parliament assists the EDPS for information technology and telephone infrastructures.

## 6.6. Administrative environment

### 6.6.1. Follow-up of the establishment of internal control standards

On the basis of the interinstitutional agreement of 24 June 2004, the internal auditor of the Commission was appointed as the auditor of the EDPS.

By his decision of 7 November 2005, and in accordance with Article 60(4) of the Financial Regulation, the EDPS established specific internal control procedures that take into account the structure, size and type of activities of the institution.

A report evaluating the internal control system was established by the EDPS services. It gives an in-depth analysis of the procedures already adopted and identifies some improvements which should be priorities in 2007. It also confirmed the functionality and efficiency of the adopted control standards as such.

The year 2006 was the first time the EDPS was subject to an internal audit. The conclusions of the audit will be summarised in a report to be produced by the internal auditor's services.

### 6.6.2. Setting up a Staff Committee

In accordance with Article 9 of the Staff Regulations of Officials of the European Communities, the Supervisor adopted on 8 February 2006 a decision setting up a Staff Committee. The Staff Committee was elected in March 2006. It was consulted on a series of general implementing provisions for the Staff Regulations and on other internal rules adopted by the institution.

### 6.6.3. Flexitime

In 2005 the EDPS adopted a decision on flexitime. This is not an obligation under the Staff Regulations; it is rather a measure to organise the working day with the aim of allowing the staff to reconcile their professional and private lives and also of enabling the EDPS to arrange working hours depending on his priorities. Every staff member is able to choose between traditional hours and flexitime, with the possibility of recovering overtime worked. This experience has demonstrated very positive results both for the institution and for the staff.

#### 6.6.4. Internal rules

The process of adopting new internal rules necessary for the proper functioning of the institution continued, as well as the adoption of new general implementing provisions for the Staff Regulations (see Annex I).

Where these provisions concern subjects on which the EDPS benefits from the assistance of the Commission, they are similar to those of the Commission, with some adjustments to allow for the special nature of the EDPS' office. These provisions are provided to new colleagues for information when they arrive. Some existing administrative procedures have been improved, and, as a consequence, the administrative guide was updated in November 2006.

An internal Data Protection Officer (DPO) has been appointed to ensure the internal application of the provisions of Regulation (EC) No 45/2001.

The EDPS started to develop some social activities (mainly child facilities such as crèches, etc.). Access of staff's children to the European School has also been guaranteed.

### 6.7. Objectives for 2007

The objectives set for 2006 were fully achieved. In 2007 the EDPS will continue the consolidation process undertaken in 2006 and develop some activities further.

The budget structure of the institution will be renewed by a new budget terminology, applicable for the establishment of the budget 2008. It will be based on the three years experience of the EDPS, taking into account the specific needs of the institution and ensuring the transparency required by the budget authority.

During 2007, the EDPS intends also to adopt new internal financial rules adapted to the size of the institution. Concerning financial software, the EDPS will make all the necessary efforts to acquire the programmes to allow the access to financial files from his premises.

A decision on staff evaluation is to be adopted in 2007, together with a guide for the evaluators. Following the adoption of these documents, the first evaluation exercise will be launched. The development of an internal training policy will be completed in 2007.

Continued administrative cooperation on the basis of the extended administrative agreement will remain an essential factor for the EDPS. In parallel, the EDPS will continue to develop the office's administrative environment and to adopt general implementing provisions for the Staff Regulations.

The mail handling will be improved with the help of the EP and the adoption of an electronic mail management system.

The implementation of the improvements identified during the first assessment of the internal control system will become a priority in 2007.

An inventory and analysis of data processing operations will be finalised during 2007 with the support of the DPO.

Aware of the degree of confidentiality required by some areas of his activities, the EDPS intends to establish a comprehensive security policy compatible with his functions.

## Annex A

## Legal framework

Article 286 of the EC Treaty, adopted in 1997 as part of the Treaty of Amsterdam, provides that Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data should also apply to 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.

### 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 now been ratified by close to 40 Member States of the Council of Europe, including all EU Member States.

Directive 95/46/EC was based on the principles of Convention 108, but specified and developed them in many ways. It aimed to provide a high level of protection and a free flow of personal data in the EU. When the Commission made the proposal for this directive in the early 1990s, it stated that Community institutions and bodies should be covered by similar legal safeguards, thus enabling them to take part in a free

flow of personal data, subject to equivalent rules of protection. However, until the adoption of Article 286 of the EC Treaty, a legal basis for such an arrangement was lacking.

The appropriate rules referred to in Article 286 of the EC Treaty have been laid down in 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<sup>(79)</sup>. This regulation has also provided for an independent supervisory authority, referred to as the 'European Data Protection Supervisor', with a number of specific tasks and powers, as envisaged in the Treaty.

The Constitutional Treaty, signed in October 2004, places great emphasis on the protection of fundamental rights. Respect for private and family life and protection of personal data are treated as separate fundamental rights in Articles II-67 and II-68 of the Constitution. Data protection is also mentioned in Article I-51 of the Constitution, in Title VI on the 'democratic life' of the Union. This clearly indicates that data protection is now 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'. This means that only activities which are totally outside the framework of the 'first pillar' are not subject to the supervisory tasks and powers of the EDPS.

<sup>(79)</sup> 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 such as 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 in fact the implementation at European level of 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 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 Community institutions and a number of 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 paragraph 2.2).

### Tasks and powers of EDPS

The tasks and powers of the EDPS are clearly described in Articles 41, 46 and 47 of the regulation (see Annex B) both in general and in specific terms. Article 41 lays down the general mission of the EDPS — to ensure that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data are respected by 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 Community 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 ‘third pillar’ (police and judicial cooperation in criminal matters). Monitoring relevant developments which may have an impact on the protection of personal data is also an important task. 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 ‘third pillar’ has a similar character. As a member of the Article 29 Working Party, established to advise the Commission and to develop harmonised policies, the EDPS has the opportunity to contribute at that level. Cooperation with supervisory bodies in the ‘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
  - 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)
    - i) 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) 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

ADS	approved destination status
ALDE	Alliance of Liberals and Democrats for Europe (political group in EP)
API	advance passenger information
CdT	Translation Centre for the Bodies of the European Union
CLP	Community <i>laissez-passer</i>
CoR	Committee of the Regions
CPVO	Community Plant Variety Office
DPC	data protection coordinator
DPA	data protection authority
DPC	data protection coordinator (only in the European Commission)
DPO	Data Protection Officer
EAS	European Administrative School
EC	European Communities
ECB	European Central Bank
ECJ	European Court of Justice
EESC	European Economic and Social Committee
EFSA	European Food Safety Authority
EIB	European Investment Bank
EMPL	Committee on Employment and Social Affairs in the European Parliament
ECHR	European Convention on Human Rights
EMA	European Medicines Agency
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EP	European Parliament
EPSO	European Personnel Selection Office
ETF	European Training Foundation
EU	European Union
EUMC	European Monitoring Centre on Racism and Xenophobia
EWS	early warning system
FP7	seventh research framework programme
IAS	Internal Auditing Service
LIBE	Committee on Civil Liberties, Justice and Home Affairs in the European Parliament
OHIM	Office for Harmonisation of the Internal Market
OLAF	European Anti-Fraud Office
PMO	European Commission Paymaster's Office
PNR	passenger name record
R & D	research and development
RFID	radio frequency identification
SIS	Schengen Information System
SWIFT	Society for Worldwide Interbank Financial Telecommunication
'Third pillar'	police and judicial cooperation in criminal matters
VIS	Visa Information System

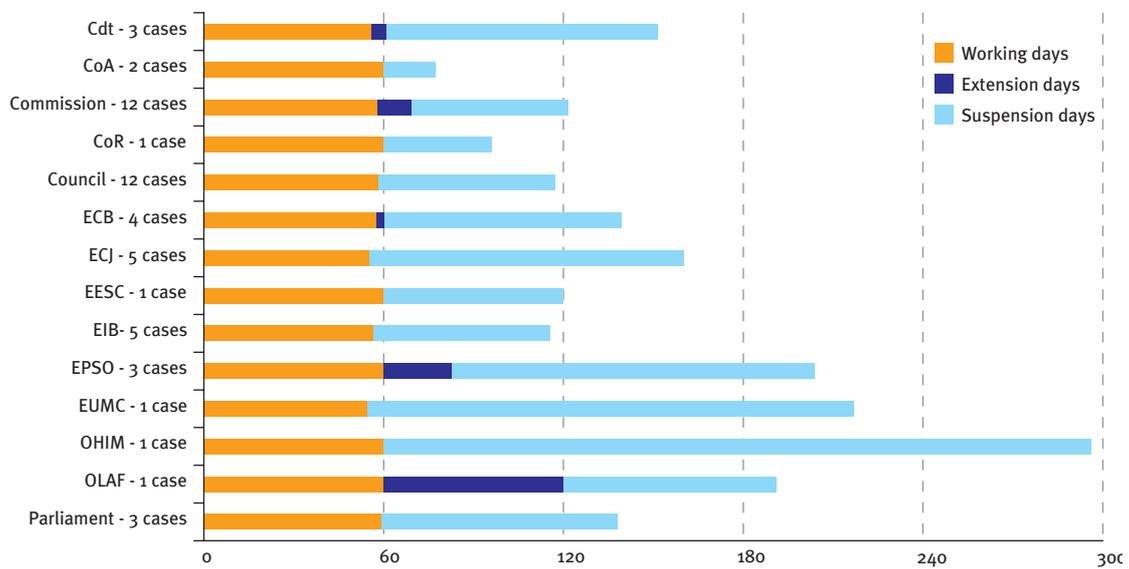
## Annex D

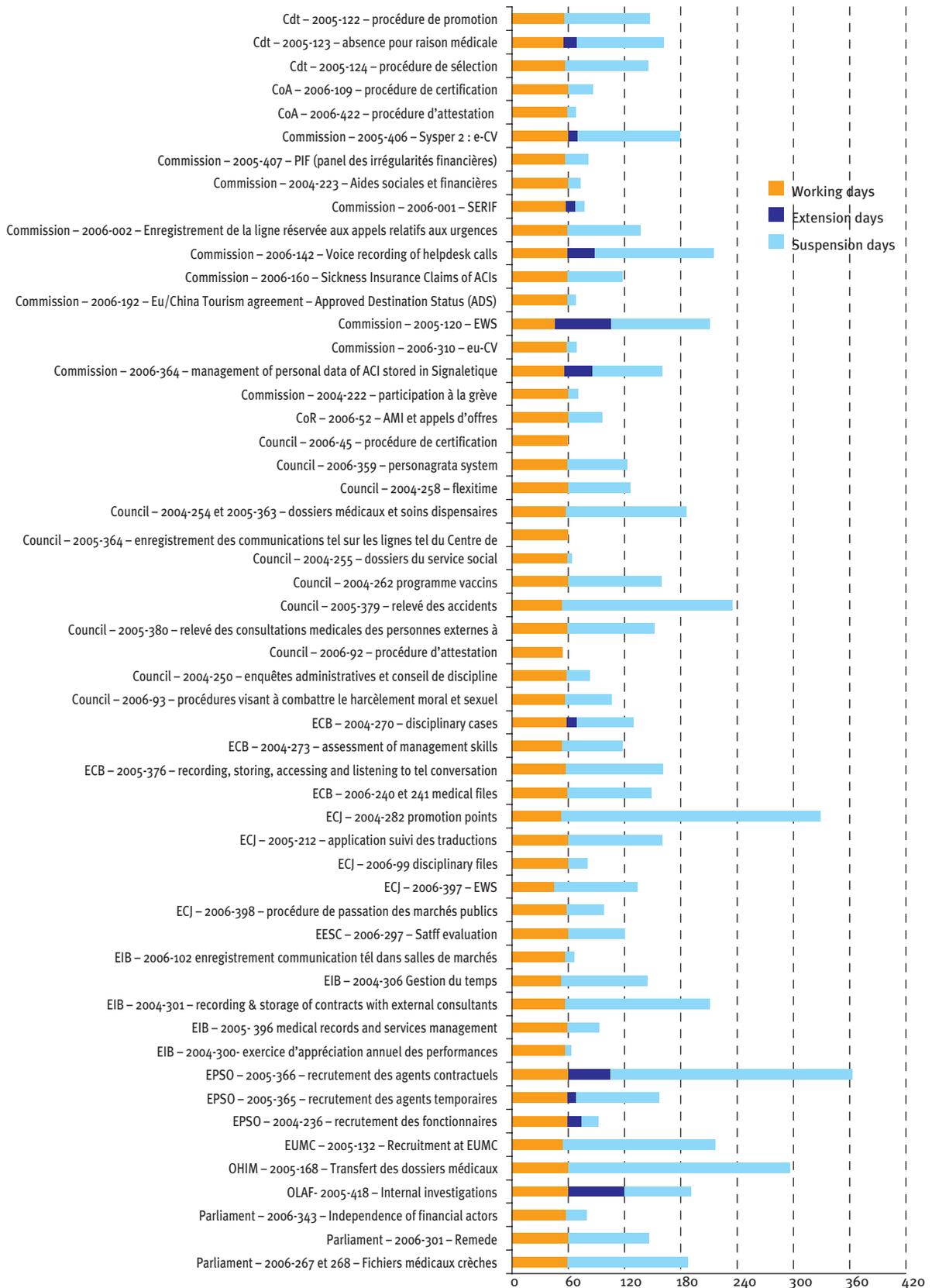
## List of data protection officers (DPO)

Organisation	Name	E-Mail
European Parliament	Jonathan STEELE	dg5data-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 Communities	Marc SCHAUSS	dataprotectionofficer@curia.europa.eu
European Court of Auditors	Jan KILB	data-protection@eca.europa.eu
European Economic and Social Committee	<i>to be nominated</i>	
Committee of the Regions	Maria ARSENE	data.protection@cor.europa.eu
European Investment Bank	Jean-Philippe MINNAERT	dataprotectionofficer@eib.org
European Ombudsman	Loïc JULIEN	dpo-euro-ombudsman@europarl.europa.eu
European Data Protection Supervisor	Giuseppina LAURITANO	giuseppina.lauritano@edps.europa.eu
European Central Bank	Martin BENISCH	dpo@ecb.int
European Anti-Fraud Office	Laraine LAUDATI	Laraine.Laudati@ec.europa.eu
Translation Centre for the Bodies of the European Union	Benoît VITALE	data-protection@cdt.europa.eu
Office for Harmonisation in the Internal Market	Luc DEJAÏFFE	dataprotectionofficer@oami.europa.eu
European Monitoring Centre on Racism and Xenophobia	Jean-Marie ADJAHÏ	Jean-Marie.Adjahi@eumc.europa.eu
European Medicines Agency	Vincenzo SALVATORE	data.protection@emea.europa.eu
Community Plant Variety Office	Martin EKVAD	ekvad@cpvo.europa.eu
European Training Foundation	Romuald DELLI PAOLI	dataprotectionofficer@etf.europa.eu
European Network and Information Security Agency	Andreas MITRAKAS	dataprotection@enisa.europa.eu
European Foundation for the Improvement of Living and Working Conditions	Markus GRIMMEISEN	dataprotectionofficer@eurofound.europa.eu
European Monitoring Centre for Drugs and Drug Addiction	Arne TVEDT	arne.tvedt@emcdda.europa.eu
European Food Safety Authority	Claus REUNIS	DataProtectionOfficer@efsa.europa.eu
European Maritime Safety Agency	Joachim MENZE	joachim.menze@emsa.europa.eu
European Agency for Reconstruction	Olli KALHA	olli.kalha@ear.europa.eu
European Centre for the Development of Vocational Training (CEDEFOP)	Spyros ANTONIOU	spyros.antoniou@cedefop.europa.eu
Education, Audiovisual, Culture	Hubert MONET	hubert.monet@ec.europa.eu

## Annex E

## Prior checking handling time per case and per institution





## Annex F

# List of prior check opinions

### **Early Warning System — Court of Justice**

Opinion of 22 December 2006 on a notification for prior checking on the early warning system (Case 2006-397)

### **Personal data of auxiliary conference interpreters — Commission**

Opinion of 22 December 2006 on a notification for prior checking on the 'Management of personal data of auxiliary conference interpreters (ACI) stored in Signalétique (application of the central database Coralin)' (Case 2006-364)

### **Crèches — Parlement**

Avis du 8 décembre 2006 sur la notification d'un contrôle préalable à propos des dossiers 'Fichiers médicaux — Crèche du Parlement' and 'Fichiers médicaux-crèches privées' (Dossiers 2006-267 and 2006-268)

### **Early warning system — Commission**

Opinion of 6 December 2006 on a notification for prior checking on the early warning system (Case 2005-120)

### **Marchés publics — Cour de justice**

Avis du 16 novembre 2006 sur la notification d'un contrôle préalable à propos du dossier 'Marchés publics' (Dossier 2006-398)

### **Remede — Parlement**

Avis du 14 novembre 2006 sur la notification d'un contrôle préalable à propos du dossier 'Remede' (Dossier 2006-301)

### **Sélection d'agents contractuels — EPSO**

Avis du 14 novembre 2006 sur la notification d'un contrôle préalable à propos du dossier 'Sélection d'agents contractuels en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires' (Dossier 2005-366)

### **PersonaGrata — Conseil**

Avis du 13 novembre 2006 sur la notification d'un contrôle préalable à propos du dossier 'PersonaGrata' (module Gestion du personnel) (Dossier 2006-359)

### **Voice recording of helpdesk calls — Commission**

Opinion of 23 October 2006 on a notification for prior checking on the 'Voice recording of Helpdesk calls' (Case 2006-142)

**Medical files — European Central Bank**

Opinion of 20 October 2006 on a notification for prior checking on medical files kept by the ECB's medical adviser and recording of medical information in the personal file (Cases 2006-240/241)

**Periodical staff reports — European Economic and Social Committee**

Opinion of 19 October 2006 on a notification for prior checking on periodical staff reports for officials and temporary agents (Case 2006-297)

**Procédure d'attestation — Cour des Comptes**

Avis du 10 octobre 2006 sur la notification d'un contrôle préalable à propos du dossier 'Procédure d'attestation' (Dossier 2006-422)

**Evaluation du risque d'indépendance — Parlement**

Avis du 25 septembre 2006 sur la notification d'un contrôle préalable à propos de l'évaluation du risque d'indépendance (Dossier 2006-343)

**Participation à la grève — Commission**

Avis du 25 septembre 2006 sur la notification d'un contrôle préalable à propos du traitement administratif générique de la participation à la grève (Dossier 2004-222)

**EU-CV online — Commission**

Opinion of 14 September 2006 on a notification for prior checking on EU-CV online (Case 2006-310)

**Sickness insurance claims — Commission**

Opinion of 28 July 2006 on a notification for prior checking on the procedure and system of 'Sickness insurance claims' related to auxiliary conference interpreters (ACIs) (Case 2006-160)

**Relevé des accidents — Conseil**

Avis du 25 juillet 2006 sur la notification d'un contrôle préalable à propos du dossier 'Relevé des accidents' (Dossier 2005-379)

**Recording and storage of contracts — European Investment Bank**

Opinion of 14 July 2006 on a notification for prior checking on 'Recording and storage of contracts concluded by and between the Bank and external consultants' (Case 2004-301)

**CIRCA website on EU-China Tourism Agreement — Commission**

Opinion of 30 June 2006 on a notification for prior checking relating to the EU-China Agreement — approved destination status (ADS) (Case 2006-192)

**Gestion du Temps — Banque européenne d'investissement**

Avis du 26 juin 2006 sur la notification d'un contrôle préalable à propos du dossier 'Gestion du temps' (Dossier 2004-306)

**Internal investigations — OLAF**

Opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations (Case 2005-418)

**'Sysper2 e-CV' — Commission**

Opinion of 22 June 2006 on a notification for prior checking on 'Sysper2- e-CV, the Commission's human capital database' (Case 2005-406)

**Harcèlement moral et sexuel — Conseil**

Avis du 9 juin 2006 sur la notification d'un contrôle préalable à propos de la réglementation interne concernant le harcèlement moral et sexuel au travail au sein du Secrétariat général du Conseil (SGC) (Dossier 2006-93)

**Disciplinary procedures — Court of Justice**

Opinion of 8 June 2006 on a notification for prior checking on data processing in the framework of disciplinary procedures (Case 2006-99)

**Dossiers médicaux / Soins dispensaires — Conseil**

Avis du 29 mai 2006 sur la notification d'un contrôle préalable à propos des dossiers 'Dossiers médicaux' et 'Soins dispensaires — main courante' (Dossiers 2004-254 et 2005-363)

**Procédure de certification — Cour des comptes**

Avis du 29 mai 2006 sur la notification d'un contrôle préalable à propos du dossier 'Procédure de certification' (Dossier 2006-109)

**Enregistrement de la ligne téléphonique réservée aux urgences — Commission**

Avis du 22 mai 2006 sur la notification d'un contrôle préalable relatif à l'enregistrement de la ligne réservée aux appels relatifs aux urgences et à la sécurité à Bruxelles (n° 88888) (Dossier 2006-2)

**Enquêtes administratives — Conseil**

Avis du 16 mai 2006 sur la notification d'un contrôle préalable à propos du dossier 'Décision concernant la conduite et la procédure des enquêtes administratives et el conseil de discipline au sein du Secrétariat général du Conseil' (Dossier 2004-250)

**Enregistrement des communications téléphoniques — Banque Européenne d'Investissement**

Avis du 8 mai 2006 sur la notification d'un contrôle préalable à propos du dossier enregistrement des communications téléphoniques dans les salles de marchés (Dossier 2006-102)

**'Programme vaccins' — Conseil**

Avis du 5 mai 2006 sur la notification d'un contrôle préalable à propos du dossier 'Programme vaccins' (Dossier 2004-262)

**Telephone monitoring — European Central Bank**

Opinion of 5 May 2006 on a notification for prior checking on the recording, storing and listening of telephone conversations in DG-M and DG-P (Case 2005-376)

**Consultation médicale — Conseil**

Avis du 4 mai 2006 sur la notification d'un contrôle préalable à propos du dossier 'Relevé des consultations médicales des personnes externes à l'institution' (Dossier 2005-380)

**Procédures d'appel à manifestation d'intérêt et d'appel d'offres — Comité des Régions**

Avis du 3 mai 2006 sur la notification d'un contrôle préalable à propos du dossier 'Procédures d'appel à manifestation d'intérêt et d'appel d'offres' (Dossier 2006-52)

**Sélection d'agents temporaires — EPSO**

Avis du 2 mai 2006 sur la notification d'un contrôle préalable à propos du dossier 'Sélection d'agents temporaires en vue de leur recrutement par les institutions européennes et le cas échéant, par les organismes, les organes ou les agences communautaires' (Dossier 2005-365)

**Medical records — OHIM**

Opinion of 28 April 2006 on a notification for prior checking on medical records (Case 2005-168)

**Absences on medical grounds — Translation Centre**

Opinion of 21 April 2006 on a notification for prior checking on the ‘Processing of absences on medical grounds and the archiving of medical certificates’ (Case 2005-123)

**Attestation procedure — Council**

Opinion of 18 April 2006 on a notification for prior checking concerning the ‘Attestation procedure’ dossier (Case 2006-92)

**Recruitment — Translation Centre**

Opinion of 10 April 2006 on a notification for prior checking relating to the ‘Selection procedure for staff recruitment (Cdt-Da-5) (Case 2005-124)

**Promotion procedure — Translation Centre**

Opinion of 7 April 2006 on a notification for prior checking regarding the ‘Promotion procedure’ dossier (Cdt-Da-3) (Case 2005-122)

**Promotions — Court of Justice**

Opinion of 7 April 2006 on a notification for prior checking on ‘Promotion points: notations and promotions’ (Case 2004-282)

**Procédure de certification — Conseil**

Avis du 23 mars 2006 sur la notification d’un contrôle préalable à propos du dossier ‘Procédure de certification’ (Dossier 2006-45)

**Reports on freelance interpreters — Commission**

Opinion of 21 March 2006 on a notification for prior checking on SERIF (‘Système d’enregistrement de rapports sur les interprètes freelance’) (Case 2006-1)

**Medical records — European Investment Bank**

Opinion of 17 March 2006 on a notification for prior checking on medical records and services management (Case 2005-396)

**Financial Irregularities Panel — Commission**

Opinion of 15 March 2006 on a notification for prior checking on the ‘Determination by the Financial Irregularities Panel (FIP) of the existence and possible consequences of financial irregularities at the European Commission’ (Case 2005-407)

**Social and financial assistance — Commission**

Opinion of 13 March 2006 on a notification for prior checking regarding social and financial assistance (Case 2004-223)

**Disciplinary cases — European Central Bank**

Opinion of 8 March 2006 on a notification for prior checking on ‘Disciplinary cases (including related administrative reviews of complaints and grievances, Ombudsman and Court cases)’ (Case 2004-270)

**Management Skills — European Central Bank**

Opinion of 7 March 2006 on a notification for prior checking on 'Assessment of management skills' (Case 2004-273)

**Recruitment by competition of permanent staff- EPSO**

Opinion of 24 February on the system of 'Recruitment, by competition, of permanent staff for the European institutions or for Community bodies, offices and agencies (Case 2004-236)

**Annual appraisal — European Investment Bank**

Opinion of 17 February 2006 on the notification for prior checking concerning the 'annual performance appraisal exercise' (Case 2004-300)

**Social services files — Council**

Opinion of 6 February 2006 on the notification for prior checking relating to the social services files (Case 2004-255)

**Recruitment — European Monitoring Centre on Racism and Xenophobia**

Opinion of 1 February 2006 on a notification for prior checking on data processing operation for recruitment (Case 2005-132)

**Recording of communications — Council**

Opinion of 23 January 2006 on the notification for prior checking relating to recordings of communications made over the Security Centre's telephone lines, building interphones and radios used by the General Secretariat of the Council (GSC) Security, Prevention and Medical Departments (Case 2005-364)

**Flexitime System — Council**

Opinion of 19 January 2006 on a notification for prior checking on the flexitime system (Case 2004-258)

**'SUIVI des traductions' — Court of Justice**

Opinion of 13 January 2006 on a notification for prior checking relating to the 'SUIVI des traductions' (Case 2005-212)

## Annex G

# List of opinions on legislative proposals

### **Financial regulation**

Opinion of 12 December 2006 on proposals for amending the financial regulation applicable to the general budget of the European Communities and its implementing rules (COM(2006) 213 final and SEC(2006) 866 final)

### **Data protection in third pillar**

Second opinion of 29 November 2006 on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

### **Mutual administrative assistance**

Opinion of 13 November 2006 on the amended proposal for a regulation of the European Parliament and the Council on mutual administrative assistance for the protection of the financial interests of the European Community against fraud and any other illegal activities

### **Common consular instructions**

Opinion of 27 October 2006 on the proposal for a regulation amending the Common consular instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications (COM (2006)269 final), OJ C 321, 29.12.2006, p. 38

### **Investigations conducted by OLAF**

Opinion of 27 October 2006 on the proposal for a regulation amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF)

### **Residence permits**

Opinion of 16 October 2006 on the modified proposal for a Council regulation amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, OJ C 320, 28.12.2006, p. 21

### ***Laissez-passer***

Opinion of 13 October 2006 on the draft Council regulation (EC) laying down the form of the *laissez-passer* to be issued to members and servants of the institutions, OJ C 313, 20.12.2006, p. 36

### **Maintenance obligations**

Opinion of 15 May 2006 on the proposal for a Council regulation on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations (COM (2005)649 final), OJ C 242, 7.10.2006, p. 20

**Exchange of information under the principle of availability**

Opinion of 28 February 2006 on the proposal for a Council framework decision on the exchange of information under the principle of availability (COM (2005)490 final), OJ C 116, 17.5.2006, p. 8

**Access to VIS by authorities responsible for internal security**

Opinion of 20 January 2006 on the proposal for a Council decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005)600 final), OJ C 97, 25.4.2006, p. 6

## Annex H

## Composition of the EDPS Secretariat

**Sectors under the direct authority of the EDPS and the Assistant Supervisor:****• Supervision**

Sophie LOUVEAUX  
*Administrator / Legal Officer*

Delphine HAROU (\*)  
*Supervision Assistant*

Rosa BARCELÓ  
*Administrator / Legal Officer*

Xanthi KAPSOSIDERI  
*Supervision Assistant*

Zsuzsanna BELENYESSY  
*Administrator / Legal Officer*

Sylvie LONGRÉE  
*Supervision Assistant*

Eva DIMOVNÉ KERESZTES  
*Administrator / Legal Officer*

Kim Thien LÊ  
*Secretariat Assistant*

Maria Veronica PEREZ ASINARI  
*Administrator / Legal Officer*

Jan DOBRUCKI  
*Trainee (March–June 2006)*

Endre SZABÓ  
*National Expert / Legal Officer*

Mate SZABÓ  
*Trainee (March–June 2006)*

Stephen McCARTNEY  
*National Expert / Legal Officer*

**• Policy and Information**

Hielke HIJMANS  
*Administrator / Legal Officer*

Per SJÖNELL (\*)  
*Administrator / Press Officer*

Laurent BESLAY  
*Administrator / Technology Officer*

Martine BLONDEAU (\*)  
*Documentation Assistant*

Bénédicte HAVELANGE  
*Administrator / Legal Officer*

Andrea BEACH  
*Secretariat Assistant*

Alfonso SCIROCCO  
*Administrator / Legal Officer*

Theodora TOUTZIARAKI  
*Trainee (October 2006–February 2007)*

Michaël VANFLETEREN  
*Administrator / Legal Officer*

---

(\*) Information team



**Personnel/Budget/Administration Unit**

Monique LEENS-FERRANDO  
*Head of Unit*

Giuseppina LAURITANO  
*Administrator / Statutory Questions  
Audit and Data Protection Officer*

Raja ROY  
*Financial and Accounting Assistant*

Vittorio MASTROJENI  
*Human Resources Assistant*

Valérie LEAU  
*Accounting Assistant*

Anne LEVÉCQUE  
*Human Resources Assistant*

Stéphane RENAUDIN  
*Trainee (October 2006–February 2007)*

Anne-Françoise Reinders  
*Human Resources Assistant*

## Annex I

# List of administrative agreements and decisions

Prolongation of the administrative agreement signed by the Secretary-General of the European Parliament, the Council and the Commission and by the European Data Protection Supervisor.

### List of service-level agreements signed by the EDPS with the other institutions

- Service-level agreements with the Commission (Traineeships Office of the Education and Culture DG; Personnel and Administration DG and Employment, Social Affairs and Equal Opportunities DG)
- Service-level agreement with the Council
- Service-level agreement with the European Administrative School (EAS)
- Administrative arrangement between the European Data Protection and the European Network and Information Security Agency (ENISA)
- Agreement on the harmonisation of the cost of the interinstitutional language courses

### List of decisions adopted by the EDPS

Decision of 12 January 2005 of the Supervisor establishing general implementing provisions on family allowances

Decision of 27 May 2005 of the Supervisor establishing general implementing provisions relating to the traineeships programme

Decision of 15 June 2005 of the Supervisor establishing general implementing provisions concerning part-time work

Decision of 15 June 2005 of the Supervisor establishing implementing provisions on leave

Decision of 15 June 2005 of the Supervisor establishing general implementing provisions on the criteria applicable to step classification on appointment or on taking up employment

Decision of 15 June 2005 of the Supervisor adopting flexitime with the possibility of making up for any overtime worked

Decision of 22 June 2005 of the Supervisor adopting common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease

Decision of 1 July 2005 of the Supervisor establishing general implementing provisions on family leave

Decision of 15 July 2005 of the Supervisor adopting common rules on sickness insurance for officials of the European Communities

Decision of 25 July 2005 of the Supervisor establishing implementing provisions concerning leave on personal grounds for officials and unpaid leave for temporary and contract staff of the European Communities

Decision of 25 July 2005 of the Supervisor on external activities and terms of office

Decision of 26 October 2005 of the Supervisor establishing general implementing provisions concerning the household allowance by special decision

Decision of 26 October 2005 of the Supervisor establishing general implementing provisions determining place of origin

Decision of 7 November 2005 of the Supervisor establishing internal control procedures specific to the EDPS

Decision of 10 November 2005 of the Supervisor laying down rules on the secondment of national experts to the EDPS

Decision of 16 January 2006 modifying of 22 June 2005 of the Supervisor adopting common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease

Decision of 16 January 2006 modifying the decision of 15 July 2005 of the Supervisor adopting common rules on sickness insurance for officials of the European Communities

Decision of 26 January 2006 of the Supervisor adopting the rules on the procedure for granting financial aid to supplement the pension of a surviving spouse who has a serious or protracted illness or who is disabled

Decision of 8 February 2006 of the Supervisor setting up a Staff Committee at the EDPS

Decision of 9 September 2006 of Supervisor adopting the rules laying down the procedure for implementing Article 45(2) of the Staff Regulations







European Data Protection Supervisor

**Annual Report 2006**

Luxembourg: Office for Official Publications of the European Communities

2007 — 91 pp. — 21 x 29.7 cm

ISBN 92-95030-12-5



## **How to obtain EU publications**

Our priced publications are available from EU Bookshop (<http://bookshop.europa.eu>), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.



Publications Office

*Publications.europa.eu*

ISBN 92-95030-12-5



9 789295 030121