

# Annual Report

**2007**



EUROPEAN DATA  
PROTECTION SUPERVISOR



# Annual Report

## 2007



EUROPEAN DATA  
PROTECTION SUPERVISOR

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, 2008

ISBN 978-92-95030-38-1

© Photos: European Parliament and iStockphoto

© European Communities, 2008

Reproduction is authorised provided the source is acknowledged.

*Printed in Italy*

PRINTED ON WHITE CHLORINE-FREE PAPER

# Contents

|   |           |
|---|-----------|
| User guide  | 6         |
| Mission statement   | 7         |
| Foreword  | 8         |
| 1. Balance and perspectives                                   | 9         |
| <b>1.1. General overview of 2007</b>                          | <b>9</b>  |
| <b>1.2. Results in 2007</b>                                   | <b>10</b> |
| <b>1.3. Objectives in 2008</b>                                | <b>11</b> |
| 2. Supervision  | 12        |
| <b>2.1. Introduction</b>                                      | <b>12</b> |
| <b>2.2. Data protection officers</b>                          | <b>12</b> |
| <b>2.3. Prior checks</b>                                      | <b>14</b> |
| 2.3.1. Legal base   | 14        |
| 2.3.2. Procedure  | 14        |
| 2.3.3. Quantitative analysis                                  | 16        |
| 2.3.4. Main issues in <i>ex post</i> cases                    | 20        |
| 2.3.5. Main issues in proper prior checks                     | 23        |
| 2.3.6. Consultations on need for prior checking               | 25        |
| 2.3.7. Notifications not subject to prior checking            | 25        |
| 2.3.8. Follow-up of prior check opinions                      | 26        |
| 2.3.9. Conclusions and future                                 | 27        |
| <b>2.4. Complaints</b>  | <b>27</b> |
| 2.4.1. Introduction   | 27        |
| 2.4.2. Cases declared admissible                              | 28        |
| 2.4.3. Cases not admissible: main reasons for inadmissibility | 31        |
| 2.4.4. Collaboration with the European Ombudsman              | 31        |
| 2.4.5. Further work in the field of complaints                | 32        |
| <b>2.5. Inquiries</b>   | <b>32</b> |
| <b>2.6. Inspection policy</b>                                 | <b>33</b> |
| 2.6.1. 'Spring 2007 and beyond'                               | 33        |
| 2.6.2. Data protection officers (DPOs)                        | 34        |
| 2.6.3. Inventory of processing operations                     | 34        |
| 2.6.4. Inventory of prior checking cases                      | 35        |
| 2.6.5. Further implementation                                 | 35        |
| 2.6.6. Conclusions  | 35        |
| <b>2.7. Administrative measures</b>                           | <b>36</b> |
| <b>2.8. E-monitoring</b>                                      | <b>38</b> |
| <b>2.9. Video-surveillance</b>                                | <b>38</b> |
| <b>2.10. Eurodac</b>  | <b>40</b> |
| 3. Consultation   | 41        |
| <b>3.1. Introduction</b>                                      | <b>41</b> |
| <b>3.2. Policy framework and priorities</b>                   | <b>42</b> |

|  |           |
|--|-----------|
| <b>3.3. Legislative opinions</b>   | <b>44</b> |
| 3.3.1. General remarks   | 44        |
| 3.3.2. Individual opinions   | 45        |
| <b>3.4. Comments</b>   | <b>51</b> |
| <b>3.5. Court interventions</b>  | <b>53</b> |
| <b>3.6. Other activities</b>   | <b>53</b> |
| <b>3.7. New developments</b>   | <b>56</b> |
| 3.7.1. Interaction with technology                                       | 56        |
| 3.7.2. New developments in policy and legislation                        | 58        |
| <b>4. Cooperation</b>  | <b>60</b> |
| <b>4.1. Article 29 Working Party</b>                                     | <b>60</b> |
| <b>4.2. Council Working Party on Data Protection</b>                     | <b>61</b> |
| <b>4.3. Coordinated supervision of Eurodac</b>                           | <b>62</b> |
| <b>4.4. Third pillar</b>   | <b>63</b> |
| <b>4.5. European conference</b>  | <b>64</b> |
| <b>4.6. International conference</b>                                     | <b>65</b> |
| <b>4.7. London initiative</b>  | <b>65</b> |
| <b>4.8. International organisations</b>                                  | <b>66</b> |
| <b>5. Communication</b>  | <b>67</b> |
| <b>5.1. Introduction</b>   | <b>67</b> |
| <b>5.2. Communication ‘features’</b>                                     | <b>67</b> |
| <b>5.3. Speeches</b>   | <b>68</b> |
| <b>5.4. Press service</b>  | <b>70</b> |
| <b>5.5. Requests for information or advice</b>                           | <b>71</b> |
| <b>5.6. Online information tools</b>                                     | <b>72</b> |
| <b>5.7. Media contacts and study visits</b>                              | <b>73</b> |
| <b>5.8. Promotional events</b>   | <b>73</b> |
| <b>6. Administration, budget and staff</b>                               | <b>75</b> |
| <b>6.1. Introduction: developing the new institution</b>                 | <b>75</b> |
| <b>6.2. Budget</b>   | <b>75</b> |
| <b>6.3. Human resources</b>  | <b>77</b> |
| 6.3.1. Recruitment   | 77        |
| 6.3.2. Traineeship programme   | 77        |
| 6.3.3. Programme for seconded national experts                           | 77        |
| 6.3.4. Organisation chart  | 78        |
| 6.3.5. Training  | 78        |
| <b>6.4. Administrative assistance and interinstitutional cooperation</b> | <b>78</b> |
| <b>6.5. Infrastructure</b>   | <b>79</b> |
| <b>6.6. Administrative environment</b>                                   | <b>79</b> |
| 6.6.1. Internal control system and audit                                 | 79        |
| 6.6.2. Staff Committee   | 79        |
| 6.6.3. Internal rules  | 80        |
| 6.6.4. Data protection officer   | 80        |
| 6.6.5. Document management   | 80        |

|   |           |
|---|-----------|
| <b>6.7. External relations</b>                                      | <b>81</b> |
| <b>6.8. Objectives for 2008</b>                                     | <b>81</b> |
| Annex A — Legal framework   | 83        |
| Annex B — Extract from Regulation (EC) No 45/2001                   | 85        |
| Annex C — List of abbreviations                                     | 87        |
| Annex D — List of data protection officers (DPOs)                   | 89        |
| Annex E — Prior checking handling time per case and per institution | 91        |
| Annex F — List of prior check opinions                              | 94        |
| Annex G — List of opinions on legislative proposals                 | 101       |
| Annex H — Composition of the EDPS Secretariat                       | 103       |
| Annex I — List of administrative agreements and decisions           | 105       |

# User guide

A mission statement and a foreword presented by Peter Hustinx, the European Data Protection Supervisor (EDPS), follow this user guide.

**Chapter 1 — Balance and perspectives** presents a general overview of the activities of the EDPS. This chapter also highlights results achieved in 2007 and puts forward the main objectives for 2008.

**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 (DPOs) in the EU administration. This chapter includes an analysis of prior checks (both quantitative and on substance), complaints (including collaboration with the European Ombudsman), inquiries, inspection policy and advice on administrative measures dealt with in 2007. Moreover, it includes sections on e-monitoring and video-surveillance, as well as an update on the supervision of Eurodac.

**Chapter 3 — Consultation** deals with developments in the EDPS' 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. It specifically deals with challenges for the existing data protection framework in the near future.

**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 EDPS' information and communication activities and achievements, as well as the work of the press service. It also runs through the use of different communication tools, such as the website, newsletters, information materials and awareness-raising events.

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

The report is completed by a number of **annexes**, which provide an overview of the relevant legal framework, the provisions of Regulation (EC) No 45/2001, a list of abbreviations and acronyms, statistics regarding prior checks, the list of DPOs of EU institutions and bodies, as well as the composition of the EDPS Secretariat and a list of administrative agreements and decisions adopted by the EDPS.

An **executive summary** of the present report is also available with a view to providing a shortened version of key developments in the EDPS' activities in 2007.

Those who wish to get further details about the EDPS are encouraged to visit our website which remains our most prominent tool of communication ([www.edps.europa.eu](http://www.edps.europa.eu)). The website also provides for a subscription feature to our newsletter.

Hard copies of the annual report as well as the executive summary may be ordered from the EDPS free of charge. Contact details are available on our website, under the 'Contact' section <sup>(1)</sup>.

---

<sup>(1)</sup> <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/12>

## Mission statement

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

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

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

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



## Foreword



It is my pleasure to submit a fourth 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 2007 as the third 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.

The Treaty of Lisbon, signed at the end of 2007, aims to ensure that the EU Charter of Fundamental Rights will be legally binding for all institutions and bodies and for the Member States when they are implementing Union law. Both instruments provide for an enhanced protection of personal data, including rules for independent supervision.

tion of personal data, including rules for independent supervision.

This is an important benchmark in the history of the European Union, but should also be understood as a challenge. The fundamental safeguards that are highlighted in the treaties have to be delivered in practice. This applies where institutions and bodies are processing personal data, but also where they develop rules and policies that may have an impact on the rights and freedoms of European citizens.

This report shows that — even under current rules in 2007 — there has been substantial progress in supervision. The emphasis on measuring results has led to investments in meeting data protection requirements in most institutions and bodies. There is reason for some satisfaction, but continued efforts are needed to come to full compliance.

In consultation, much emphasis has been put on the need for a consistent and effective framework for data protection, both in the first and in the third pillar, but not always with satisfactory results. The report shows at the same time that an increasing variety of policy areas benefits from the consultative activities of the EDPS.

Let me therefore take this opportunity, once again, to thank those in the European Parliament, the Council and the Commission who support our work, and many others in different institutions and bodies who are directly responsible for the way in which data protection is delivered in practice. Let me also encourage those who are 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. The qualities that we enjoy in the staff are outstanding and have continued to contribute greatly to our effectiveness.

Peter Hustinx  
*European Data Protection Supervisor*

# 1. Balance and perspectives

## 1.1. General overview of 2007

The legal framework within which the European Data Protection Supervisor (EDPS) acts <sup>(2)</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>(3)</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 2007 are presented. The importance of information and communication about these activities fully justifies a separate emphasis on communication in Chapter 5. Most of these activities rely on effective management of financial, human and other resources, as discussed in Chapter 6.

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

<sup>(3)</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)

The Treaty of Lisbon, signed on 13 December 2007, marked the end of a reflection on the role, structure and functioning of the European Union. On 12 December 2007, a slightly revised version of the EU Charter of Fundamental Rights was signed in Strasbourg. Although the charter is no longer part of the treaty, it will be legally binding for all EU institutions and bodies and for the Member States when they are implementing Union law. The protection of personal data, including the need for independent supervision, is clearly visible in both instruments and is designed to have a horizontal impact. The EDPS will closely follow the developments in this area in the near future.

The enhanced protection of personal data, as provided for in the Lisbon Treaty, is also an opportunity for institutions to show how to deliver this protection in practice. The EDPS has emphasised from the outset that many EU policies depend on the lawful processing of personal data, and that effective protection of personal data, as a basic value underlying EU policies, should be seen as a condition for their success. The EDPS will continue to act in this general spirit and is pleased to see that it is finding increasing support.

Prior checking continued to be the main aspect of supervision during 2007. The 'spring 2007' deadline set by the EDPS to measure compliance with Regulation (EC) No 45/2001 has resulted in an impressive increase of the number of notifications submitted for prior checking, and therefore also of the number of relevant opinions issued by the EDPS. The total number of admissible complaints has also increased considerably. All Community institutions and bodies, including recently established agencies, have now ensured the appointment of an internal data protection officer (see Chapter 2).

The consultative activities continued to develop well. Great emphasis was put on the need for a consistent and effective framework for data protection, both in the first and in the third pillar. However, in the latter case, the results have not been satisfactory. Further to the inventory of Commission proposals, published at the end of 2006, the EDPS has dealt with an increasing variety of policy areas, which resulted in more opinions, comments and other activities at different stages of the legislative process. A number of interesting court cases has also required attention (see Chapter 3).

Cooperation with national supervisory authorities has focused on the role of the Article 29 Working Party, which resulted in the adoption of important documents on strategic issues. The EDPS has played a key role in the coordinated supervision of Eurodac. This approach will be of value for other large-scale information systems. Much attention has also been given to an improved cooperation in third pillar matters. Finally, the EDPS has invested in the follow-up of the 'London initiative' which is designed to raise awareness of data protection and to make it more effective (see Chapter 4).

## 1.2. Results in 2007

The 2006 annual report mentioned that the following main objectives had been selected for 2007. Most of these objectives have been fully or partially realised.

- **Scope of DPO network**

The network of data protection officers (DPOs) has reached its full scope, with all institutions and bodies taking part in its activities, including all Community agencies. The EDPS has continued to give strong support and guidance to the development of DPO functions, with a particular emphasis on newly appointed DPOs.

- **Continue prior checking**

The number of prior checks relating to existing processing operations has increased remarkably, but most institutions and bodies still have some work ahead in meeting their obligations in this area. Results of prior checks are regularly shared with DPOs and other relevant parties.

- **Inspections and checks**

The EDPS has started measuring progress in implementation of Regulation (EC) No 45/2001 as from

spring 2007. All institutions and bodies have been involved in this exercise, but attention has been given to their particular phase of development. The results have been reported, both in general and case by case, and are summarised in Chapter 2.

- **Video-surveillance**

The EDPS has completed surveys of video-surveillance practices both at EU level and in the Member States, and dealt with different cases involving individual institutions or bodies. This experience will provide the basis for draft guidelines to be published for consultation on the EDPS website in 2008.

- **Horizontal issues**

Opinions on prior checks and decisions on complaints are continuously analysed for horizontal issues. The first papers with guidance for all institutions and bodies will be published in 2008. Issues relating to the conservation of medical or disciplinary data have been discussed with appropriate authorities.

- **Consultation on legislation**

The EDPS has continued to issue opinions on proposals for new legislation and has ensured adequate follow-up. The advisory role covers a wider area of subjects and is built on a systematic inventory and selection of priorities, prepared with the full support of relevant Commission services and currently in its second year.

- **Data protection in third pillar**

The EDPS has continued to give special attention to the development and adoption of a general framework for data protection in the third pillar. He has also regularly dealt with proposals for the exchange of personal data across borders, particularly in the context of the Prüm Treaty. In both cases, this had unfortunately only limited impact.

- **Communicating data protection**

The EDPS has given strong support to follow-up activities of the 'London initiative' aimed at 'communicating data protection and making it more effective'. This involved activities to share 'best practices' in enforcement and strategic development with data protection authorities from different countries around the world.

- **Rules of procedure**

The preparation of rules of procedure, covering the different roles and activities of the EDPS, has taken

more time than expected. However, the development of different internal case manuals has made good progress. Rules of procedure will be adopted and published in the course of 2008, together with practical information for interested parties on the website.

- **Resource management**

The EDPS has improved the management of financial and human resources, by a renewal of the budget structure, adoption of internal rules on evaluation of staff and development of a training policy. The implementation of an internal control system and the appointment of a data protection officer have been further improvements.

### 1.3. Objectives in 2008

The following main objectives have been selected for 2008. The results achieved on them will be reported next year.

- **Support of DPO network**

The EDPS will continue to give strong support to internal data protection officers, particularly for recently established agencies, and will encourage a further exchange of expertise and best practices among them.

- **Role of prior checking**

The EDPS intends to finish prior checking of existing processing operations for most institutions and bodies, and put emphasis on the implementation of recommendations. Results of prior checks and follow-up will be shared with DPOs and other relevant parties.

- **Horizontal guidance**

The EDPS will develop guidance on relevant issues common to most institutions and bodies (e.g. processing of health-related data, providing access to data subjects and dealing with video-surveillance). Guidance will be made widely available. A series of seminars will be organised for interested parties.

- **Measuring compliance**

The EDPS will continue to measure compliance with Regulation (EC) No 45/2001, with different kinds of checks for all institutions and bodies, and increasingly execute inspections on the spot. The EDPS will also publish a general inspection policy.

- **Large-scale systems**

The EDPS will further develop a coordinated supervision of Eurodac, together with national supervisory authorities, and develop expertise required for the supervision of other large-scale systems, such as SIS II and VIS, in the near future.

- **Opinions on legislation**

The EDPS will continue to issue timely opinions or comments on proposals for new legislation, on the basis of a systematic inventory of relevant subjects and priorities, and ensure adequate follow-up.

- **Treaty of Lisbon**

The EDPS will continue to follow developments with regard to the Lisbon Treaty and will closely analyse — and where necessary advise on — its impact for data protection.

- **Online information**

The EDPS intends to update and increase the information available on the website and to further improve the electronic newsletter.

- **Rules of procedure**

The EDPS will adopt and publish rules of procedure, covering his different roles and activities. Practical tools for interested parties will be available on the website.

- **Resource management**

The EDPS will consolidate and further develop some activities relating to financial and human resources, and enhance other internal work processes. Additional office space will be required to accommodate future staff.

## 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). Regulation (EC) No 45/2001 ('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 2007. 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 the regulation. 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 has prior checked existing processing operations in most relevant categories. Special attention has been given to interinstitutional systems and other situations of joint use by institutions and bodies, with a view to streamlining and simplifying procedures. The EDPS' opinions allow controllers to adapt their processing operations to comply with the regulation. The EDPS also has other methods at his disposal such as the handling of complaints, inquiries, inspections and advice on administrative measures.

As regards the powers vested in the EDPS, during 2007 as in previous years, there has been no need to order, warn or ban, as controllers have implemented the EDPS' recommendations or expressed the intention of doing so and are taking the necessary steps. The promptness of the responses differs from one case to



Assistant Supervisor Joaquín Bayo Delgado.

another. The EDPS has developed a systematic follow-up to the recommendations.

### 2.2. Data protection officers

The regulation provides that at least one person should be appointed as data protection officer (DPO) in each Community institution and body (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.





Data protection officers during their 20th meeting in Brussels (8 June 2007).

For a number of years, the DPOs have met on a regular basis in order to share common experiences and discuss horizontal issues. This informal network has proved productive in terms of collaboration. This has continued during 2007.

In 2007, the DPO of Europol was accepted into the network, with the status of observer.

The EDPS attended a part of each of the meetings held between the DPOs in March 2007 (EMSA, Lisbon), June 2007 (Council, Brussels) and October 2007 (Office for Harmonization in the Internal Market — OHIM, Alicante). 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 issues raised in the framework of the prior checking work. In particular, the scope of Article 27 was further defined, namely with examples such as electronic communication systems, internal audit systems and investigations carried out by DPOs. The meetings also granted 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 paragraph 2.3).

The EDPS made use of the DPO meetings to provide DPOs with information on the 'spring 2007' inspection

exercise (see paragraph 2.6.1). The purpose of the exercise was explained, its methodology was described and the targeted actions which may follow were outlined. The DPO meetings were also a good opportunity for the DPOs to give feedback on the impact of the exercise within their own institution or agency, and enabled the EDPS to take certain factors into account.

A 'DPO quartet' composed of four DPOs (Council, European Parliament, European Commission and OHIM) was set up with the aim of coordinating the DPO network. The EDPS has closely collaborated with this quartet, notably to prepare the agendas of meetings.

Back to back with the June meeting in Brussels, a workshop for the new DPOs was organised by the EDPS in collaboration with 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. The main tasks of a DPO were also explained and a presentation was made of the notification forms, registers of notifications to the DPO and IT tools.

The working group on time limits for conservation of data, on blocking and on erasure met for six working meetings during 2007. The Assistant EDPS and two staff members participated in these meetings. A draft paper on the conclusions of the work of the subgroup

has been drafted and will be circulated in 2008 by the members of the working group to chosen persons in their institution or body (IT specialists, for example). A document on the relevant rules on time limits and blocking was also prepared and discussed by the members of the group.

In the framework of the 'spring 2007' exercise, the EDPS underlined the legal obligation for each EU institution or body to appoint a DPO (see paragraph 2.6.1).

## 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 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 <sup>(4)</sup>;

---

<sup>(4)</sup> *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 previous years 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 7 to 10 days <sup>(5)</sup>) 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.

For *ex post* cases received before 1 September 2007, the month of August was excluded from calculations both for institutions/bodies and the EDPS, taking into account the huge quantity of cases (see the chart in paragraph 2.3.3).

---

<sup>(5)</sup> Working days, when they coincide with holiday periods.

## 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 is about to be made available on the new website of the EDPS, together with a summary of the case.

## 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. Only in two opinions issued in 2007 (proper prior checking cases 2007-373 and 2007-680, see below), were the conclusions different: the processing operations were in breach of the regulation and some recommendations had to be implemented to bring them into compliance.

For the first time in 2007 changes in previously prior checked operations have been notified. An abbreviated form of opinion has been developed for those cases.

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' opinions are adopted following 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 to a particular case are followed up and, where applicable, that all enforcement decisions are complied with (see paragraph 2.3.7).

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

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 under way 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 has requested the





Supervision team during a meeting.

DPOs to analyse the situation of their institution concerning processing operations within the scope of Article 27 since 2004. Following the receipt of contributions from all DPOs, a list of cases subject to *ex post* 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:

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

These categories were used in 2005 and 2006 as priority categories, but in order to give full effect to the deadline of 'spring 2007' they were not applicable any more for prioritisation and rather used only for systematic control. Proper prior checking cases have never been subject to these categories, as they must be dealt with before the processing operation is implemented.

### 2.3.3. Quantitative analysis

#### Notifications for prior checking

As mentioned both in the 2005 and 2006 annual reports, the EDPS has constantly encouraged DPOs

to increase the number of prior checking notifications to the EDPS.

The deadline of spring 2007 for receipt of notifications to be prior checked by the EDPS — *ex post* cases — was fixed to trigger Community institutions and bodies to increase their efforts towards a complete fulfilment of their notification obligation.

The effect was a significant increase of notifications: 132 notifications between 1 January 2007 and 30 June 2007, compared with 137 in total until then (32 in the second half of 2006), plus 44 notifications during the second half of 2007. The real effect of 'spring 2007' was therefore 208 (132 + 32 + 44) notifications out of a total of 313 between 2004 and the end of 2007.

#### Opinions on prior checking cases issued in 2007

In 2007, **90 opinions** <sup>(6)</sup> on prior checking notifications were issued.

These 101 cases finalised with a formal opinion represent an increase of 77.19 % of work in prior checking compared with 2006. This workload is without a doubt linked to the 'spring 2007' deadline <sup>(7)</sup>.

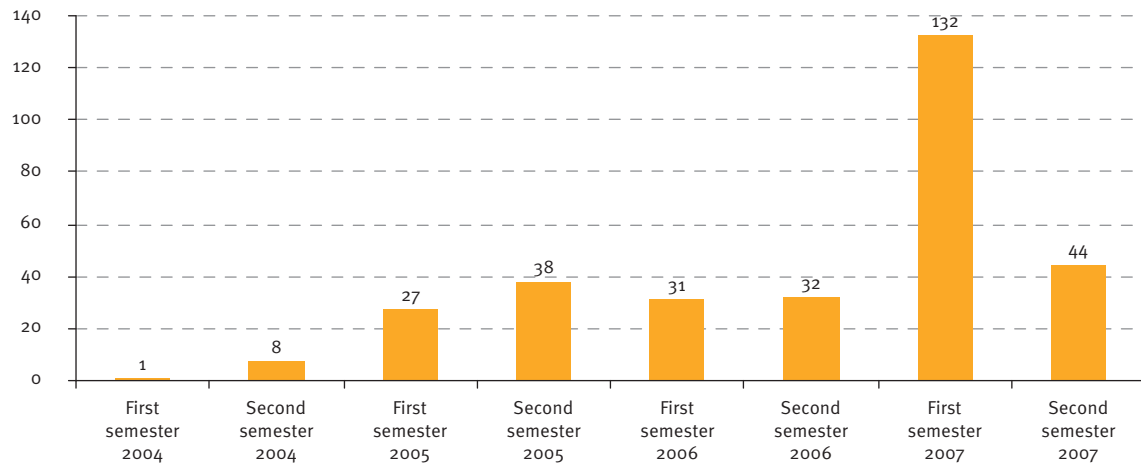
Out of the 101 prior checking cases (90 opinions), 11 were proper prior checking cases, i.e. the institutions concerned (one each for the ECA, Parliament, EPSO, European Ombudsman, ETF, ECB, EIB and OLAF and three for the Commission) followed the procedure involved for prior checking before implementing the processing operation:

- 4 of those 11 prior checking cases (the three of the Commission and one from the ETF) were related to the flexitime system;

<sup>(6)</sup> Out of 101 notifications, for practical reasons and due to the fact that some cases were linked, 15 notifications of OLAF were treated jointly in four different opinions. This is why 101 notifications resulted in 90 opinions.

<sup>(7)</sup> See paragraph 2.3.7 for the other 31 cases finalised during 2007.

## Notifications at the EDPS



|  |                           |
|--|---------------------------|
| Council of the European Union                                    | 3 cases                   |
| European Commission  | 19 cases                  |
| European Central Bank (ECB)                                      | 5 cases                   |
| Court of Justice   | 5 cases                   |
| European Investment Bank (EIB)                                   | 1 case                    |
| European Parliament  | 11 cases                  |
| Translation Centre for the Bodies of the European Union (CdT)    | 1 case                    |
| European Personnel Selection Office (EPSO) (*)                   | 1 case                    |
| European Court of Auditors (ECA)                                 | 3 cases                   |
| Committee of the Regions (CoR)                                   | 4 cases                   |
| European Ombudsman   | 7 cases                   |
| Office for Harmonization in the Internal Market (OHIM)           | 7 cases                   |
| European Anti-Fraud Office (OLAF)                                | 25 cases<br>(14 opinions) |
| Community Plant Variety Office (CPVO)                            | 1 case                    |
| European Food Safety Authority (EFSA)                            | 1 case                    |
| European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) | 1 case                    |
| European Medicines Agency (EMA)                                  | 2 cases                   |
| European Maritime Safety Agency (EMSA)                           | 2 cases                   |
| European Training Foundation (ETF)                               | 2 cases                   |

(\*) EPSO relies on the DPO of the Commission.

- 2 of those 11 were related to incompetence of staff;
- the others were related to the need for a third language for promotion, management of leave, security clearance rules, medical records and services management and fraud notification system (see also paragraph 2.3.5).

It should be noted that the two processing operations which were in breach of the regulation are within those 11 proper prior checking cases (one related to a specific flexitime, the other to medical records). The remaining 90 cases (79 opinions) were *ex post* prior checking cases.

In addition to these 101 cases on which an opinion has been issued, the EDPS has also dealt with 31 cases which were found not to be subject to prior checking. Among this relatively high quantity of those so-called 'non-prior checks' (23.48 % of the global quantity of the 132 cases finalised in 2007), 11 of them belong to the e-monitoring category. The analysis of these 31 cases is developed in paragraph 2.3.7.

### Analysis by institution/body

Most institutions and bodies have notified processing operations likely to present specific risks. The important effort in issuing prior checking opinions made during 2007 is the follow-up of the notification effort of DPOs. The European Commission made important progress in this field, although a significant number of notifications are still to be received. The European Parliament, OLAF and the European Ombudsman also appear with significant numbers. As regards EU agencies, OHIM has been very active in notifying processing operations. Some other agencies have slowly started to notify processing operations. The related opinions will be issued in 2008 (see below 'Notifications for prior checking received before 1 January 2008 and pending' and paragraph 2.6).

### Analysis by category

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

|  |          |
|--|----------|
| Category one (medical files)             | 16 cases |
| Category two (staff appraisal)           | 41 cases |
| Category three (offences and suspicions) | 14 cases |
| Category four (social services)          | 8 cases  |
| Category five (e-monitoring)             | 4 cases  |
| Other areas                              | 7 cases  |

**Category one** includes the medical file itself and its different contents (five cases), sick leave (three cases), invalidity procedure (one case), day-nurseries (one case), sickness schemes (one case), radiation dosimetry (one case) and four cases linked to health-related data. This category has decreased in percentage (26.5 % of cases in 2005, 24.6 % of cases in 2006, 17.77 % of cases in 2007) but has given the EDPS the opportunity to advise on the content of medical files. In 2007 the EDPS analysed a case linked to radiation dosimetry at the Joint Research Centre, which will be followed by some others.

The major category theme remains the **second category**, relating to the evaluation of staff (41 files out of the 90), with a relatively stable percentage (56 % of cases in 2005, 40.4 % in 2006, 45.55 % in 2007). Ten cases were linked to recruitment (of trainees, of seconded national experts, of senior officials, recruitment at the ECB and at CPVO), five cases were linked to evaluation, three to promotions, two to incompetence of staff (both proper prior checking cases), eight to certification and attestation procedures, four to flexi-time (all proper prior checking cases), two to early retirement and seven to various others matters.

Regarding the **third category** (relating to offences and suspected offences), a significant increase of cases (14 opinions, which represents 15.55 % of the total) took place but it should be underlined that this category includes nearly all the cases from OLAF (see paragraph 2.3.4). Only two opinions were issued on disciplinary procedures as most institutions had already notified those cases in previous years.

Regarding the **fourth category** (social services), the number of notifications has multiplied by four (eight opinions, which represents 8.88 % of the global amount of opinions). All major institutions have complied with notifications in this area, as well as OHIM.

It appears that most agencies are not in a position to offer those kinds of services to their own staff.

Regarding the **fifth category** (e-monitoring), only four opinions were issued, as most notifications related to e-monitoring have been considered by the EDPS as non-prior checking cases due to the fact they did not present specific risks (breach of confidentiality under Article 27.1 of the regulation, or suspected offences under Article 27(2)(a), or evaluation of personal aspects according to Article 27(2)(b)). Analysis by the EDPS, however, led to numerous recommendations (see paragraph 2.3.7).

Regarding the notifications which do not belong to those categories, the EDPS has continued analysing the area of financial matters such as PIF (Financial Irregularities Panel — Parliament and Court of Justice), the early warning system (Parliament and OLAF) and the procurement procedure (Council). The other matters are participation in a strike (Council) and security clearance rules (ECB).

### Timelines of the EDPS and the institutions and bodies

The three charts in Annex E illustrate the timelines of the EDPS and of the Community institutions/bodies. They detail the number of days needed for the EDPS for drafting opinions, 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 days of the EDPS for drafting opinions:* this represents a decrease of 1.73 %, or one day less than in 2006 (55.5 days in 2005, 57.9 in 2006 and 56.9 in 2007). It is a very satisfactory figure considering the increase of numbers and complexity of the notifications sent to the EDPS.

*Number of extension days for the EDPS:* this represents a decrease of 15.74 %, nearly one day less than in 2006 (3.3 days in 2005, 5.4 days in 2006 and 4.55 days in 2007). Although the maximum extension can reach two months (Article 27.4 of the regulation), it has been normally less than a month.

*Number of suspension days:* since mid-2006, this includes the suspension for 7 or 10 days for comments and further information from the DPO on the final

draft. In *ex post* cases received before 1 September 2007, the month of August has not been included in the calculation. The increase between 2006 (average of 72.8 days per file) and 2007 (average of 75.14 days per file) is 3.21 %. Taking into account that, in 2005, the average was of 29.8 days per file, the EDPS is concerned about the lengthy periods needed by the institutions/bodies to complete information, especially in three cases (185, 200 and 203 days respectively). 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:* for 2007, the charts show that some institutions and bodies have increased their suspension days very significantly (such as the European Parliament, CoR, ECA, CdT and some others to a lesser extent, such as the ECB and the Commission), while others have succeeded in decreasing them (such as OHIM, EIB, Court of Justice, Council).

#### Notifications for prior checking received before 1 January 2008 and pending

By the end of 2007, **69 prior checking cases** were in process. Of these, 4 notifications were sent in 2006 and 65 notifications in 2007. Of these 69 pending cases, 25 were already finalised with an opinion by the end of February 2008.

|                  |          |
|------------------|----------|
| OLAF             | 4 cases  |
| Parliament       | 4 cases  |
| Council          | 9 cases  |
| Commission       | 23 cases |
| ECB              | 1 case   |
| EESC and CoR     | 3 cases  |
| EIB              | 3 cases  |
| ECA              | 2 cases  |
| Court of Justice | 2 cases  |
| Ombudsman        | 1 case   |
| Cedefop          | 1 case   |
| CPVO             | 2 cases  |
| EFSA             | 1 case   |
| EMCDDA           | 1 case   |
| EMEA             | 7 cases  |
| EMSA             | 2 cases  |
| EPSO             | 1 case   |
| OHIM             | 1 case   |
| CdT              | 1 case   |

#### Analysis by institution and body

As said before the result of the 'spring 2007' deadline, more agencies have started the process of notifying (Cedefop, EMCDDA, EMEA — especially with seven notifications — and EMSA) or continued to do so (CdT, EFSA and CPVO). The EDPS encourages the other agencies and bodies to do likewise.

Council and Commission numbers are also important. As for the Commission, 16 of those 27 are from the different Joint Research Centre (JRC) sites and mainly deal with two matters — radiation dosimetry and access control — due to the very specific context of the JRC (one of the directorates in the Research DG, with a high degree of autonomy).

#### Analysis by category

The number of notified prior checking cases by category pending on 1 January 2008 was as follows:

|  |          |
|--|----------|
| Category one (medical files)             | 20 cases |
| Category two (staff appraisal)           | 25 cases |
| Category three (offences and suspicions) | 4 cases  |
| Category four (social services)          | None     |
| Category five (e-monitoring)             | 3 cases  |
| Other areas                              | 17 cases |

In **category one**, the continuing process of notifications leads to the following remarks:

- this category represents 28.98 % of those pending at the beginning of 2008;
- one case, the medical file of the Commission, plays an interinstitutional role on specific aspects (e.g. archiving of medical files);
- among those 20 prior checking cases, eight are from different JRC sites and in different areas such as the individual medical file (for all JRC sites), first aid and accidents, sick leave, invalidity procedure, and three relating to radiation dosimetry;
- the EDPS welcomes the fact that notifications in this area are also being received from agencies such as CPVO and EMEA;
- the EDPS is still waiting for the Office for the Administration and Payment of Individual Entitlements (PMO) notification as mentioned in the previous annual report.

The **second category** theme (staff appraisal) still represents the majority of cases — exactly one third. Eight of

those cases relate to recruitment procedures (use of the reserve lists of EPSO by institutions) and to recruitment procedures by agencies. All pending evaluation procedures concern agencies (EMCCDA, CPVO, EMEA, EMSA and EFSA). Two other notifications deal with flexitime (see paragraph 2.3.5). The year 2008 will also be the first occasion for the EDPS to analyse a notification in the area of training policy (Council 2007-584).

Regarding the **third category** (offences and suspected offences), the EDPS is dealing with OLAF cases and the disciplinary procedure and administrative inquiries of Cedefop. The EDPS encourages the other agencies to notify their cases.

Concerning **category four** (social services), the EDPS is not surprised to have no pending notifications as agencies have explained in the context of 'spring 2007 and beyond' (see paragraph 2.6) that they are very often not in a position to offer those kinds of services to their personnel.

**Category five** (e-monitoring) is still of particular importance. In 2007, the EDPS organised several meetings about e-monitoring and set up an interactive exercise about raising awareness on this subject. The conclusions of this exercise will be summarised in conclusions to be published in 2008.

**Other areas** (24.63 % of the cases) involve three main fields: calls for tenders, video-surveillance and access control systems. The last two areas are of particular importance: a video-surveillance paper will be issued in 2008 (see paragraph 2.9) and access control is a highly sensitive subject, sometimes involving radio frequency identification (RFID) technology or biometrics. In addition, the EDPS will have the first occasion to issue an opinion about 'politically exposed persons' at the European Investment Bank, a matter also of high sensitivity.

### 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 directly or indirectly to the state of health of an individual fall under this category. Therefore, recording of sick leave and sickness insurance claims are also subject to prior checking. In this category areas such as invalidity procedure, radiation dosimetry and nurseries were also examined by the EDPS.

These different prior checking cases have given the EDPS the occasion to analyse in depth issues relating to the processing of medical data by the Community institutions and agencies. The relevance of some of the questions raised in the pre-employment and annual medical visits has been questioned by the EDPS in the light of the purpose of these visits. The preventive role of the pre-employment medical exam has been examined by the EDPS, who recommends that this exam does not, in principle, seek any preventive purposes without the consent of the data subject. The EDPS has also requested that questions about family members with no genetic link to the person concerned be removed from the medical questionnaires.

The EDPS considers that the annual medical check-up should be considered as a preventive service, but only based on the consent of the person concerned. The annual medical check-ups must not normally serve to certify fitness for work, although specific testing and certification is permitted in limited and clearly defined cases, for example if the employee is exposed to dangerous substances.

Conservation periods for medical data have also been the object of recommendations in EDPS prior checking opinions in the light of the opinion of the EDPS delivered to the College of the Heads of Administration (2006-532) <sup>(8)</sup>. Notably, medical data collected during the pre-recruitment medical visit concerning non-recruited candidates should only be kept for a set period of time.

The issue of the data quality of the medical file has also been raised in the framework of different prior checking cases. The EDPS has concluded that, although it is difficult to speak of accuracy of medical data, the principle of data quality notably entitles the data subject to request that the medical opinion of another doctor or any other relevant information is added to the file to ensure that the data are updated.

A particular issue relating to the transfer of personal data was raised in the framework of the prior checking opinion on the reimbursement of medical expenses (Commission 2004-238). In the context of an appeals procedure foreseen by Article 90(2) of the Staff Regulations of Officials of the European Communities, the EDPS recommended removing identification infor-

---

<sup>(8)</sup> See EDPS 2006 annual report, p. 35. See also common conservation list in paragraph 2.7 below.



mation in the transmission of data to the Management Committee as it is unnecessary in order for the Committee to provide its reports.

**Recruitment** is a common processing operation in all institutions and bodies for obvious reasons. In 2006 the interinstitutional recruitment procedure carried out by EPSO was examined and gave rise to an opinion by the EDPS (2004-0236). In 2007, the Parliament and the ECB notified for prior checking the processing of personal data about the use of these EPSO reserve lists. OLAF also notified its recruitment procedure for temporary agents from specific reserve lists. The proportionality of OLAF's policy regarding staff security clearance was questioned notably as regards staff members who do not need to have access to highly classified information based on applicable Community legislation.

The EDPS also prior checked the Commission procedure for recruitment of senior officials (2007-0193). In his opinion, the EDPS recalls that candidates should be able to have access to their entire file, comprising the grids and assessment notes concerning them drafted by the various committees competent for their assessment. The EDPS is aware that there is a limitation to this rule; this is the principle of the secrecy of selection committees' proceedings, as set out in Article 6 of Annex III to the Staff Regulations. In accordance with Article 20(1)(c) of the regulation, no marks given by individual members of the committee should be given and information comparing the data subject with other applicants should not be provided.

**Staff evaluation:** The Commission 'Sysper 2 promotions' case was the occasion to issue recommendations related to data retention and to request the Commission to evaluate the need to mention any pending disciplinary procedure in the system as a cause for suspension of the promotion exercise <sup>(9)</sup>.

The certification and attestation procedures have continued to be sent to the EDPS by various institutions and agencies. The recommendations issued by the EDPS relate notably to data conservation periods, taking into account legal remedies and new applications by the same persons.

<sup>(9)</sup> Furthermore, in relation to a complaint (case 2007-529, see below), the EDPS has been able to issue another recommendation relating to the fairness of the processing, asking for a more detailed procedure relating to 'priority points'.



Medical files always contain sensitive data.

Two prior checking opinions refer to the early retirement procedure at the Commission (2006-577) and at OHIM (2007-575). In other areas, recommendations relate to the data conservation period and to the right of access of the data subject to the report of the committee responsible for determining those persons entitled to early retirement, subject to certain restrictions according to Article 20(1)(c) of the regulation. The necessity of the publication of the reserve list of persons requesting early retirement was also questioned by the EDPS.

Lastly, in the various areas of staff evaluation, some opinions have been issued relating to a study on stress at work at OHIM, special advisers, special indemnities, election observation roster and redeployment exercise.

**OLAF procedures:** The EDPS issued 12 opinions concerning the OLAF procedures (one of which is a true prior check (fraud notification system, see paragraph below 2.3.5)). One opinion (joint cases 2006-544, 2006-545, 2006-546, 2006-547) dealt

with judicial, disciplinary, administrative and financial follow-up. The four data-processing operations concern the processing of personal data that take place within the third stage of OLAF investigations, the so called 'follow-up phase' ensuring that the competent Community and/or national authorities have implemented the measures recommended by OLAF. In general, the procedures comply with the principles established in the data protection regulation. However, the EDPS did make some recommendations mainly as concerns the necessity of certain data introduced in the system, the obligation to establish the necessity of data transfers and the information provided to data subjects. The EDPS also requested that the 20-year conservation period be evaluated by OLAF when OLAF reaches 10 years of existence. The EDPS underlined that the recommendations made in his opinion should be taken on board when updating the OLAF case manual.

Another opinion dealt with all external investigations and operations (2007-047, 048, 049, 050 and 072). External investigations are administrative investigations outside the Community organs and are performed for the purpose of detecting fraud or other irregular conduct of natural or legal persons affecting the financial interests of the European Communities. The results of OLAF's external investigations are referred to the appropriate national or Community authorities for judicial, administrative, legislative or financial follow-up. The EDPS notably asked OLAF to attach a note to the file establishing the necessity of the transfer of personal data in a given case and to ensure the right of access and rectification of one's own personal data as a main rule. In this respect, OLAF has to ensure that any restriction under Article 20 of the regulation on the right of access to one's own personal data and/or the right to rectify them should meet a necessity test applied on a case-by-case basis, and that due respect is given to Article 20(3)(4) and (5) of the regulation. Furthermore, OLAF must respect the confidentiality of whistleblowers and informants during OLAF external investigations.

The EDPS has also prior checked the processing activities conducted by OLAF's Supervisory Committee (SC) (2007-0073). The purpose of such processing is to reinforce OLAF's independence by regular monitoring of the implementation of the investigative function, as required by Article 11 of Regulation (EC) No 1073/99. The EDPS has recommended, among other

points, that the SC must have access to the case management system (CMS) files (ongoing, closed and non-cases) only on a case-by-case basis. When such access is requested, a note should be included in the CMS file specifying the reasons that justify the provision of access. Moreover, the SC must respect Article 12 of the regulation regarding the persons concerned, including whistleblowers, witnesses and informants.

In sum, the EDPS has conducted a thorough analysis of OLAF's processing activities in the field of data related to suspected offences, and issued recommendations where necessary. Some further examples are the following:

- fraud notification system (2007-481);
- information and intelligence data pool and intelligence databases (joint cases 2007-027 and 2007-028);
- criminal assistance cases (2007-203);
- customs information system (2007-177);
- anti-fraud information system (AFIS) (joint cases 2007-084, 2007-085, 2007-086, 2007-087);
- free phone service (2007-003).

**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.

A number of prior checking opinions were issued by the EDPS in this area. The EDPS notably recommended that the social worker who processes the personal data must be properly informed of the requirement to comply with the principle laid down in Article 4(1)(c) of the regulation, namely that the data processed must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. This principle must be complied with in relation to the data supplied by the applicant and the social worker's personal notes.

A recurrent recommendation in the prior checking opinions on social services concerned the extreme care needed in all communications of the social worker with external services, because of the nature of the data being transferred. The EDPS also specified that the right of rectification in the framework of the social files held by the social worker notably implies the right

for the data subject to give his or her point of view, especially when the subjective evaluation of the social worker could have certain consequences on the exercise of the rights of the person concerned.

**E-monitoring:** Despite the fact that the EDPS has not yet adopted his final position on e-monitoring (see paragraph 2.8 below), several opinions in this area were adopted. Two opinions were issued relating to the ECB investigation procedure on the use of office phones and business mobile phones (2004-271 and 2004-272). Both opinions included a recommendation related to the period of conservation of traffic data that should not, in principle, be longer than six months subject to certain specific exemptions. Traffic data can be processed for statistical purposes, but in such cases must be rendered anonymous.

The EDPS also issued an opinion regarding the silent monitoring of professional communications to the OHIM switchboard and Information Centre (2007-128) on a selective basis (two or three times a year) notably to assess the quality of the service provided, increase customer satisfaction and ultimately provide training to new staff members. The EDPS considered that the processing could be based on Article 5(a) of the regulation as, in principle, it could be considered as necessary for the purposes described, with some nuances as to the training. The EDPS also stressed that a method to guarantee the accuracy of the data should be developed.

Many cases notified to the EDPS in relation to e-monitoring were declared non-eligible for a prior checking as the data were merely processed for billing and traffic management and were not linked to specific risks or suspected offences or evaluation (see paragraph 2.3.7).

(Regarding video-surveillance, see paragraph 2.9.)

### 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, 11 cases of 'proper' <sup>(10)</sup> prior checking were notified to the EDPS in 2007. Among those 11 cases, two are

<sup>(10)</sup> That is, cases concerning a processing operation not yet implemented.

related to incompetence of staff and four to flexitime.

The European Court of Auditors has set up a procedure to deal with signs of incompetence of its staff and to remedy the problem (case 2006-534). The EDPS' analysis has primarily led to recommendations concerning information that must be provided to staff members, mainly with reference to the specific decision and to the data protection implementing decision of the Court, as well as to the setting of data retention time limits. The recommendations relating to the European Parliament case (2006-572) were made on several points, including the storage of data related to completed or interrupted remedial procedures, or on the processing of health-related data in this context.

**Time management systems** have been of significance in 2007. The EDPS received the general notification from the Commission (case 2007-063) for 'time management', a module of Sysper 2 (staff management system), which integrates 'flexitime', followed by specific flexitimes from two DGs (case 2007-218 for the Information Society and Media DG and case 2007-680 for the Agriculture and Rural Development DG), which were both adaptations of the master notification. They were eligible for prior checking on the grounds of Articles 27(2)(a) (health-related data) and 27(2)(b) (processing intended to evaluate staff efficiency, competence and ability to work).

'Time management' of the Commission was a proper prior check only as concerns the **flexitime** part and led, among others, to recommendations on the use of the staff personal number, to guarantee consistency in the system, on the information as to the mandatory or voluntary nature of data gathered from the staff members, and on the distinction in the total credit time.

The Information Society and Media DG added to the flexitime application an additional and important component in the form of an RFID chip integrated in the personal badge necessary to clock in and out. The inclusion of such a technology into a flexitime system reinforces the specific risks already present in the system. In his conclusions, the EDPS requested several modifications to the planned system regarding security aspects by introducing an interim solution, as well as concerning the drafting of the privacy statement, some organisational measures and the data subjects concerned.





Time management systems reveal data on behaviour and other personal aspects.

Regarding the specific flexitime of the Agriculture and Rural Development DG, the EDPS has considered this notification to be in breach of Regulation (EC) No 45/2001, as the expected purpose (to open to several people within a unit — far more than the head of unit — the possibility to identify absence of personnel in order to replace them as soon as possible) could be reached by other less intrusive means. Furthermore, the purpose presented by the Agriculture and Rural Development DG could not be reached by the proposed flexitime system.

The fourth case about time management was sent by ETF (case 2007-209). The time-recording database is intended to provide ETF management with information about how much time was spent on the accomplishment of the various tasks and projects by the various individuals and teams. The main recommendations were on data quality, which was very difficult to ensure given the way the system was set up, and on purpose limitation, namely that the information had to be only used for the management of a project and not for individual appraisal.

Another proper prior check opinion was released on an issue relating to time management, namely the EIB case about medical records and time management (case 2007-373). Initially, it was sent as a consultation as to the need for prior checking, as there were two previous opinions (2005-396 'Medical records' and 2004-306 'Time management') and the intention of the EIB was to allow access to all data related to uncertified sick leave kept in the 'time management' tool by the physician at the Occupation Health Centre (OHC). This was the first time that the EDPS had to issue a new opinion based on changes made to the object of a previous prior checked case.

In his opinion, the EDPS expressed that the EIB would be in breach of certain provisions of the regulation (lawfulness of the processing, data quality principle, processing of special categories of data) unless it ensures that staff members are requested to provide their freely given, unambiguous consent to the OHC physician's access to data regarding their uncertified medical leave. When requesting consent, it must be ensured that the staff member clearly understands that consent can be withheld or subsequently withdrawn at any time, without any justification, and with no adverse consequences. It must also be made clear that providing this information will only serve the purposes of prevention.

Among the other proper prior checking cases, the EDPS underlines the following cases:

- the EPSO case (2007-088) about the evaluation of the capacity to be able to work in a third language, which includes a recommendation on the automatic correction by processors;
- the Ombudsman case (2007-134) about management of leave, with some recommendations on health-related data and information to data subjects;
- the ECB case (2007-371) about security clearance rules (data-processing activities which the ECB carries out in the context of running security clearance procedures in order to ascertain whether or not a person is eligible for a security clearance), where the excessiveness of data has to be avoided; and
- the OLAF case (2007-481) about a fraud notification system (web-based information system that OLAF has put at the public's disposal in order to facilitate the collection of information to use in the fight against fraud, corruption and other illegal activities affecting the financial interests of the

Community), with two crucial issues: information to persons concerned by information received and protection of informants and whistleblowers.

### 2.3.6. Consultations on need for prior checking

During 2007, the number of consultations on the need for prior checking by the EDPS increased significantly: 20 consultations in 2007 compared with 15 in 2006. Several cases referred to above were previously subjects of consultation, namely: 'Medical records and time management', 'Flexitime — Information Society and Media DG', 'Data processed by social counsellor', 'Redeployment exercise', etc.

Other cases which have been declared subject to prior checking such as 'Annual prize', 'Security investigations', 'Freelance consultants', 'Use of EPSO reserve list', 'Audit reconciliation tool' and 'EFSA experts database' have not yet been formally notified to the EDPS following his feedback on the need to prior check.

The processing operation relating to 'politically exposed persons' at the EIB was considered as subject to prior checking as it includes data on criminal convictions or on suspicions of criminal offences.

The 'Rules regarding entry to OHIM buildings of children of staff' case has been specific in the sense that, initially considered subject to prior checking, the case has been withdrawn. The rules have indeed been changed by the agency in a way that they do not involve the processing of personal data any more.

The processing operation on the management of Internet access at the Court of Justice was not concluded to be prior checkable. Indeed, it did not aim to evaluate conduct or there was no breach of confidentiality of communications.

On the same ground, the 'telephony' processing operation at the Council was not considered as being subject to prior checking as it did not involve a breach of the confidentiality of communications.

Another interesting decision in this field has been the case of the Court of Justice on the e-mail system. The system is not subject to prior checking as no regular or random monitoring has been put in place for the

misuse of the electronic messaging system. There is no processing operation intended to evaluate personal aspects such as ability, efficiency or conduct.

Although the 'travel arrangements' processing operation at the Council might involve data relating to health, it was not concluded to be prior checkable. The purpose of the processing clearly does not aim at the processing of medical data which only comes into question in certain isolated cases and with the consent of the data subject.

### 2.3.7. Notifications not subject to prior checking

In 2007 the EDPS also dealt with 31 cases which were found not to be subject to prior checking (23.48 % of the cases finalised by the EDPS). This conclusion has been reached after a careful analysis of the notification.

Nevertheless, this analysis leads in most cases to some recommendations of the EDPS. Eleven of these cases relate to e-monitoring, two to flexitime, four to access control, and the rest either to the area of personnel (initial grading, identity cards, external activities' request, renewal of contracts, insider trading rules) or to various other areas such as accreditations or investigations by the DPO from OLAF.

As to the **e-monitoring** category, most of those notifications<sup>(1)</sup> have been notified to the EDPS for prior checking on the basis of Article 27.1 of the regulation.

It should be reminded that electronic communications can be subject to prior checking by the EDPS under two main scenarios:

- Article 27(1) of the regulation subjects to prior checking all processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. Chapter IV of the regulation contains a particular provision on the confidentiality of communication (Article 36). Where there is a breach of confidentiality of com-

<sup>(1)</sup> Notifications related to e-mail system or telephony (EESC and CoR 2006-507 and 2006-508), to telephone and fax infrastructure, network and system, to Internet statistics, to telephone calls database, to telephone billing (Commission, cases 2007-358, 2007-359, 2007-367 and 2007-374), to fixed telephony and mobile telephony (Court of Justice, cases 2007-438 and 2007-439), to register of telephone calls (EIB, case 2004-302) and to invoicing for private use of services' GSMs (OLAF, case 2007-204).

munication, a specific risk to the rights and freedoms of data subjects may exist, and, therefore, the processing operation is subject to prior checking by the EDPS;

- Article 27(2) of the regulation contains a non-exhaustive list of processing operations that are likely to present specific risks. The list includes, inter alia:
  - processing of data ‘relating to suspected offences or offences or security measures’ (Article 27(2)(a));
  - processing operations ‘intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct’ (Article 27(2)(b)).

Where a mechanism is in place to monitor the communication network for purposes of Articles 27(2)(a) and/or 27(2)(b) of the regulation, the processing operations must be submitted to the EDPS for prior checking.

This means that not all electronic communication systems are necessarily subject to prior checking. In fact, if the confidentiality of communications is not breached and the IT infrastructure is not used to monitor employee conduct, there is often no reason to submit the electronic communication systems for prior checking.

Having said that, the EDPS has nevertheless issued recommendations related to the retention periods for traffic and billing data, as provided for by Article 37(2) of the regulation, and also to information to be given to data subjects,

Regarding **access control**, three notifications<sup>(12)</sup> were submitted under Article 27(2)(b) of the regulation. After analysis, the EDPS concluded that there was no evaluation at all in those contexts. Nevertheless, recommendations were made about the exact purpose of the processing. The fourth case<sup>(13)</sup> was notified under Articles 27(2)(a) and 27(2)(d), but those were not applicable in that specific case. Article 27(2)(a) was indeed only triggered under exceptional circumstances and the list of exclusions, not being set up by the controller of the processing operation, made Article 27(2)(d) not applicable.

---

<sup>(12)</sup> Commission (2007-375, 2007-376 and 2007-381).

<sup>(13)</sup> Commission (2004-235).

The two cases related to **time management**<sup>(14)</sup> were considered non-eligible for prior checking as there was no evaluation of staff but rather an evaluation of OLAF or JRC activities. The processing of information for the purposes of monitoring activities of an EU institution with the aim of better planning the resource allocation does not fall within the criteria of Article 27(2) of the regulation. Many recommendations for the JRC case were made about purpose limitation, data quality, information to be given to data subjects and data retention period.

### 2.3.8. Follow-up of prior check opinions

When the EDPS delivers a 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 issued when a case is analysed to decide on the need for prior checking and some critical aspects appear to deserve corrective measures. Should the controller not comply with these recommendations, the EDPS may exercise the powers granted to him under Article 47 of the regulation. The EDPS may in particular refer the matter to the Community institution or body concerned, and take further steps to ensure compliance. Should the decisions of the EDPS not be complied with, he has a right to refer the matter to the Court of Justice 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, up to now, 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 formal letters sent together with his opinions, that the institution inform the EDPS of the measures taken to implement the recommendations within a period of three months.

During 2007, the EDPS closed 38 cases, which represents more than the double of 2006, certainly due to the systematic follow-up of all recommendations.

---

<sup>(14)</sup> Commission time accounting system JRC (2007-503) and OLAF time management system (2007-300).

### 2.3.9. Conclusions and future

It is clear that prior checks, both 'proper' and *ex post*, have continued to be a major activity in the supervision task of the EDPS. It was strategically decided from the very beginning that the *ex post* application of Article 27 of the regulation would be an excellent way of monitoring European institutions and agencies as to their processing of personal data in the most risky areas, and it has proved to be so.

Conclusions for 2007 can be summarised as follows:

- the 'spring 2007' deadline has given rise to a tremendous increase of notifications from many DPOs, especially during the first semester of the year, in which more than 42 % of the total of notifications (132 out of 313, from 2004 to 31 December 2007) were received;
- this has put a great amount of pressure on the supervision team at the EDPS, with a very satisfactory outcome, as the number of opinions prepared has not meant any change in the period taken to prepare opinions (including extension days) and quality has been respected;
- there is still much to improve in the periods that institutions and agencies take to answer the requests for further information from the EDPS;
- with no specific priority areas in *ex post* cases, there has been a significant broadening of topics under the scrutiny of the EDPS (time management, OLAF cases, interinstitutional processing, etc.);
- as in the previous year, two opinions reached the conclusion that the concerned cases were in breach of the regulation and that important changes had to be introduced to comply with data protection rules;
- recommendations have continued to focus mainly on data retention, the right of information and the right of access.

Future efforts will concentrate on the following points:

- institutions should finalise their *ex post* notification process and agencies should make a substantive step towards the same goal in 2008;

- the follow-up of recommendations will continue to take place systematically through information from the controller, and will be combined with on-the-spot inspections; these will also include the full implementation of the notification process to the DPO and the full compliance with the obligation of notifying proper prior check cases to the EDPS before the processing operation starts;
- some areas, such as video-surveillance, will benefit from a new approach, based on standard setting and submission for prior checking of deviating cases only;
- the criteria developed so far will be summarised by category in order to ensure consistency in all opinions and to give guidance to institutions and bodies regarding their implementation of data protection rules.

## 2.4. Complaints

### 2.4.1. Introduction

Article 41(2) of the regulation 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>(15)</sup>.

Any natural person may lodge a complaint with the EDPS, with no conditions of nationality or place of residence, on the basis of Articles 32 and 33 of the regulation <sup>(16)</sup>. Complaints can also be introduced by members of staff of the European institutions and

<sup>(15)</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>(16)</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'.

agencies to whom the Staff Regulations apply, on the basis of Article 90(b) of the Staff Regulations <sup>(17)</sup>.

Complaints are only admissible if they emanate from a natural person and relate to 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 detailed below, a number of complaints filed with the EDPS were declared inadmissible because they fell 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 also requests that the complainant inform him on other possible actions before a national court, the Court of Justice or the Ombudsman (whether pending or not).

If the case is admissible, the EDPS proceeds 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 access to all personal data and to all information necessary for the inquiry from the controller or the concerned institution/body. He can also be granted access to any premises in which a controller or institution/body carries out its activities.

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. In that case, the EDPS can:

- order the controller to comply with requests to exercise certain rights of the data subject;
- warn or admonish the controller;
- order the rectification, blocking, erasure or destruction of all data;
- impose a ban on processing;
- refer the matter to the Community institution concerned, or to the Parliament, the Council and the Commission;
- refer a matter to the Court of Justice <sup>(18)</sup>.

---

<sup>(17)</sup> Any person to whom the Staff Regulations apply may submit to the EDPS a request or a complaint within the meaning of Article 90(1) and (2), within his sphere of competence.

<sup>(18)</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.

In 2007, the EDPS received 65 complaints. Out of these 65 cases, 29 were declared admissible and further examined by the EDPS. A number of these are briefly examined below.

#### 2.4.2. Cases declared admissible

##### Collection of excessive data relating to visitors

The EDPS received a complaint from a person visiting the European Commission as part of a visiting group, concerning the publication of the passport number and date of birth of each member of the group (case 2006-0578). After investigation, the EDPS concluded that this was excessive as not in accordance with the principle of data adequacy laid down in Article 4(1)(b) and 4(1)(c). Following the EDPS investigation, such a practice has stopped and the EDPS was therefore satisfied that the matter was concluded. The EDPS took the occasion of the complaint to remind the Commission of its obligation to provide certain information to group leaders or coordinators so as to ensure the fair processing of the data.

A complaint was also received in relation to the processing of personal data by the European Parliament in connection to the attendance to a hearing (case 2007-0430). The complainant was requested to provide certain details for the purpose of attending a hearing, such as her name and date of birth. When she turned up at the hearing, she was shocked to find that the date of birth of each participant was shared with everyone as part of a list of delegates handed out during the meeting. After investigation by the EDPS, it was concluded that such data was necessary for the issuance of badges by the security unit of the Parliament but that, indeed, the data should not necessarily have been distributed to all participants and that this will be closely examined in the future.

##### Access to data

The EDPS received a complaint from a junior expert working in a European Commission delegation concerning his limited access to his personal file in violation of Article 13 of the regulation (case 2007-0127). The complainant also complained about the fact that



the Commission contacted his previous employers without his consent, thereby not informing him of the sources of the data, and contested the forwarding of his personal data by the External Relations DG to the Commission delegation for which he worked.

After investigating the facts, the EDPS concluded that certain restrictions to the right of access were justified on the basis of Article 20(1)(c), notably when necessary to protect previous employers. As to contacting his previous employers without his consent, the EDPS concluded that since the complainant himself provided full details about his previous employers and signed an application form stating that the information he provided was true, complete and correct, it was reasonable to assume that the employer could contact previous places of employment to confirm the statements made in his application. Finally, as regards the transfer of data from the External Relations DG to the Commission delegation, the EDPS concluded that the transfer was necessary for the legitimate performance of the tasks carried out by the Commission delegation in accordance with Article 7(1) of the regulation.

The complainant had also introduced a complaint to the European Ombudsman. The EDPS therefore passed on the results of his investigations to the European Ombudsman so as to avoid duplication of their investigation.

Another complaint was received from a civil servant from the Commission who claimed his right of access to the *procès verbal* (PV) established following the interview in which he took part for his current job (case 2007-0250). In this context, the right of access is to be understood as the access to the complainant's personal data contained in the PV of the assessment panel. After investigations, the EDPS found out that no PV had been established, and that consequently no personal data in the context of the assessment of the oral interview were recorded. Therefore the right of access under Article 13 of the regulation could not have further effect. The EDPS closed the case underlining that it was a general principle of good administration that the final assessment of an oral interview/test was recorded.

A complaint was lodged against the European Commission concerning the right of access to preparatory documents relating to the attribution of priority points

(in the framework of the promotion procedure) (case 2007-0529). Access was denied on the basis of the Staff Regulations, taking into consideration the confidentiality of the proceedings of the jury.

The conclusion of the EDPS was that Article 6 of Annex III of the Staff Regulations (secrecy of proceedings of the jury) had to be interpreted jointly with Article 20(1)(c) of the regulation. The independence and liberty of directors are not threatened by the right of access of the data subject, but the data should not allow any linkage to an identifiable person. These conclusions were nevertheless not applicable to the complaint as the documents had since been destroyed and so the Commission was not in a position to give access to them. The EDPS therefore asked for a new detailed notice about attribution and management of priority points to fulfil Articles 4(1)(a) (fairness) and 12 (information to be given) of the regulation.

A complaint was made against the European Court of Auditors concerning a person's right of access under Article 13 to staff assessments and to the documentation which would support the staff reports, as well as to possible secondary personal files (case 2006-597).

After further requests for clarification of the situation to both the controller and the complainant, the EDPS concluded that the assessment procedure at the European Court of Auditors (prior checked by the EDPS in case 2005-0152) did not require any documentation to support the statements made in the evaluation reports. Moreover, the EDPS did not find evidence that secondary personal files existed. Finally, regarding the request of blocking of data, the EDPS considered that none of the conditions of Article 15 of the regulation for blocking applied in the case.

#### **Forwarding and copying of e-mails**

A complaint against OLAF was received concerning the fact that an e-mail of the complainant addressed to a staff member of OLAF on a personal basis was forwarded to her head of unit and deputy head of unit (case 2007-0188). The EDPS concluded that, since there was no indication in the e-mail that this was a personal message, the concerned member of OLAF handled it in accordance with OLAF internal rules. As a consequence, the competence of the recipients as such was not in breach of the regulation.

The same complainant also complained that the response he received from OLAF was copied to a broad range of persons in violation of Article 7(1) of the regulation. The EDPS accepted that Article 7(1) allows for the transfer of certain data if the data are necessary for the legitimate performance of a task covered by the competence of the recipient. However, he took the view that, in the present case, this had not been clearly justified for all the persons put in copy. Furthermore, any transfer must comply with the other provisions of the regulation and, in particular, the data subject must be made aware of the recipients and categories of recipients (Article 11(1)(c)), which was not the case.

The EDPS is presently working with OLAF to avoid a repetition of this type of action.

#### **Requirement of credit card details**

A complaint was lodged with the EDPS by two members of staff of the European Parliament regarding the requirement of the personal or business credit card number to guarantee the booking of missions (case 2007-0338). After investigations by the EDPS, it appeared that the European Parliament did not require a credit card to process bookings for hotels and neither did the accredited travel agency. However, hotels do require the credit card number to guarantee a booking. The only cases when the Parliament does require such a number is when a staff member is unable to book a room within the financial limits laid down and must produce the costs from the accredited travel agency by means of a reservation form, which includes the credit card number. The Parliament has, however, since proceeded to remove the section carrying the credit card number from the reservation form.

As to the use of a corporate card, this depends on a personal choice of the individual staff member. Any processing of personal data in relation to the corporate credit card therefore relies on the unambiguous consent of the staff member and is legitimate under Article 5(d) of the regulation.

#### **Processing of sensitive data**

The EDPS received a complaint from an ECB employee claiming the improper processing operation of data relating to health in the framework of management of sick leave (case 2007-0299). The

complainant considered that the special category of personal data in the terms of Article 10(1) of the regulation had been processed without sufficient grounds for necessity according to Article 10(2)(b). After having analysed the facts, the EDPS concluded that the ECB was entitled to use the exception laid down in Article 10(2)(b). This conclusion was drawn on the basis that the processing of the data was necessary for the purposes of complying with the specific rights and obligations of the controller in the field of applicable employment law.

#### **Right of rectification**

A complaint on the right of rectification of a civil servant of the Commission was pending at the end of 2006 (case 2006-0436). In 2007, the EDPS received the confirmation that an interim solution had been put in place to allow the plaintiff to complete his personal data in his career background (*historique de carrière*) in Sysper2. The Commission also explained why the blocking of the complainant's personal data would have had as a consequence the interruption of every processing operation of the plaintiff in Sysper2, such as, for instance, the payment of his salary. The EDPS closed the complaint but opened a new case to follow up the technical explanation about the difficulties of the Commission to rectify and block the personal data in the Sysper2 database.

A complaint was received from a person who claimed that the word 'invalidity' was mentioned in all her pension statements from 9 November 2006 onwards. The divulgence of her data relating to health caused her a lot of inconvenience with three banks. Subsequent to the filing of a complaint to the EDPS, the Personnel and Administration DG finally erased the word 'invalidity' from her pension statement.

#### **Obligation to provide information**

A complaint was submitted by a data subject against OLAF (case 2007-0029). The complainant stated that data related to him, and not obtained from him, were collected, stored and transferred to third parties in the framework of an OLAF Final Case Report, without informing him accordingly (Article 12 of the regulation). The data subject also complained on the basis of Article 13 of the regulation. Indeed, having requested OLAF to have access to his data, a copy of the OLAF Final Case Report was received, but with

all personal data having been removed, including his own data. Furthermore, the complainant stated that he believed that OLAF's Final Case Report gave a selective and tendentious presentation of his behaviour, and he therefore wanted to exercise the right of rectification (Article 14 of the regulation).

After having evaluated the case, the EDPS noted that OLAF had not respected the obligations imposed by Articles 11 and 12 of the regulation. Furthermore, the EDPS held the view that the complainant had to receive a copy of the Final Case Report where any processing of personal data relating to him could be seen, in order to comply with Article 13 of the regulation (blackout passages containing his personal data should be avoided). Finally, the EDPS pointed out that he would evaluate the request of rectification after access had been provided, and in case the complainant maintained his submission in this regard.

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

On 1 July 2005, the EDPS received a complaint against OLAF which raised various issues under the regulation, notably unfair processing of personal data and transfer of incorrect data concerning the complainant by OLAF, in the context of an investigation into his alleged involvement in a case of bribery, in the course of 2002 and in early 2004 (case 2005-0190).

On 1 December 2005, the Assistant EDPS adopted a decision on the complaint. Although accepting that the EDPS was competent to hear the complaint, in so far as it raised issues that are within the scope of Regulation (EC) No 45/2001, it concluded that no further action could be taken by the EDPS, which would alter the situation in a fruitful way. This case was briefly mentioned in the 2005 annual report.

In 2006, the complainant lodged a complaint to the European Ombudsman about the way in which his initial complaint had been dealt with. In a second complaint, he also objected to the brief presentation of his case in the 2005 annual report, stating that it had been incorrect and premature. As to the second complaint, the EDPS accepted to provide an appropriate update on the case, with a correct and complete description of the complainant's case, as presented above. The first complaint was still before the European Ombudsman in early 2008.

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

Out of the 65 complaints received in 2007, 36 were declared not admissible as they fall outside of the area of competence of the EDPS. The vast majority of these complaints did not concern personal data processing by an EC institution or body but exclusively related to processing at national level. Some of these complaints called for the EDPS to reconsider a position taken by a national data protection authority, which falls outside of his mandate. In such cases, the complainants were informed that the European Commission would be competent in case a Member State fails to implement Directive 95/46/EC correctly.

#### **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 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.

In order to avoid unnecessary duplication and to ensure a consistent approach to both general and specific data protection issues raised by complaints, a memorandum of understanding (MoU) was signed in November 2006 between the Ombudsman and the EDPS. In practice, the memorandum has led to useful sharing of information between the EDPS and the Ombudsman whenever relevant. The Ombudsman has consulted the EDPS on cases where data protection issues were at stake and has informed the EDPS of his decisions relating to cases which either had also been submitted to the EDPS or had data protection implications. In one complaint case in which the complainant had also chosen to introduce a complaint to the Ombudsman, the results of the inquiry carried out by the EDPS were forwarded to the Ombudsman so as to avoid duplication of investigations.





Nikiforos Diamandouros, Joaquín Bayo Delgado and Peter Hustinx during an informal meeting.

The EDPS advised the Ombudsman on several complaints relating to the access to documents, in accordance with Parts C and D of the MoU. Observations were sent to the Ombudsman who included them in his decisions. These complaints allowed the EDPS to further develop his policy on the balance between public access and data protection, on the EDPS Background Paper of 2005 (published on the website), in cases where there is a clear public interest in access to information. The complaints included requests for access to additional pension schemes for Members of Parliament (MEPs), the accounts of all MEPs of one Member State and on the extension of the secondment of an official (within the Commission).

#### 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, together with information on the admissibility of complaints, will be made available on the EDPS website in due course.

Staff members also participated in the national data protection authorities' case-handling workshops in Helsinki in April 2007 and in Lisbon in November 2007. During these workshops, the EDPS gave presentations on public access to documents and data

protection in the EU administration and on OLAF internal investigations and forensic examination of computers.

The EDPS also made the most of these workshops to share experience and gather information on ongoing data protection issues in the national context. Among others, the EDPS raised the issue of the implementation in the Member States of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing relevant in a pending prior checking case.

## 2.5. Inquiries

Article 46(b) of the regulation provides that the EDPS can conduct inquiries, also at his own initiative. The EDPS conducted a number of such inquiries, some of which merit special attention in this report (see also paragraph 2.9 on video-surveillance).

### OLAF security audit

In 2007, the EDPS received numerous notifications from OLAF dealing with data-processing activities which run on the same IT infrastructure. These tools, which were initially hosted by the data centre of the European Commission, are now transferred to the OLAF premises and are managed directly by OLAF staff.

In order to ensure a consistent approach to OLAF's security measures, the EDPS decided to launch a security inspection and analysed them in a horizontal way, rather than doing it in the context of each particular prior checking notification. Conducting this analysis with a dedicated security inspection also contributed to a better handling of the confidentiality dimension of these security measures.

The main objective of the inspection was to gather facts on the implemented or forthcoming security and data protection measures, and compare them with the requirements in that field in order to assess their compliance with legal and technical standards.

After having provided guidance for the improvement of the systems through recommendations, the EDPS concluded that he was, generally speaking, very satisfied with the security measures implemented by OLAF

on the IT systems and applications under its responsibility.

The efficiency of the implementation of these security measures will be assessed in 2008 with an in-depth security audit foreseen by OLAF, to which the EDPS will be associated as an observer.

## SWIFT

On 1 February 2007, the EDPS issued his opinion on the role of the ECB in the SWIFT case (US authorities accessing banking data in the fight against terrorism). The opinion focused on the role of the ECB as an overseer, a user and a policymaker.

At the same time, in the context of the coordinated action of EU data protection authorities, the EDPS also requested the main Community institutions to provide clarifications on payment systems used and on contractual relations with SWIFT.

On 14 February 2007, the European Parliament adopted a joint resolution on passenger name record (PNR) and SWIFT. With regard to SWIFT, the European Parliament endorsed the EDPS opinion and called on the ECB and other relevant institutions to ensure that European payment systems fully comply with European data protection law.

During spring 2007, further to the EDPS requests, the ECB presented a report concerning the measures taken to comply with the opinion while other institutions provided clarifications with regard to the respect of data protection rules in their payment systems.

On the basis of the information received, the EDPS recommended to relevant Community institutions measures to ensure that they fully comply with their legal obligations under Regulation (EC) No 45/2001, in particular that they provide sufficient information to staff members and other individuals having contractual relations with them.

In a broader perspective, as a member of the Article 29 Working Party, the EDPS closely followed the progress achieved in this case, such as:

- SWIFT's adhesion to the Safe Harbor, to cover the transfers for commercial purposes to the US operating centre;

- the clarifications and assurances provided by the US Treasury concerning essential aspects — for example, the purposes, proportionality, supervision and redress mechanisms — with regard to access and processing of SWIFT data further to subpoenas;
- the important changes announced, in the longer term, to the architecture of SWIFT payment services: a new operating centre located in Switzerland will ensure that intra-European messages remain in Europe and are no longer mirrored in the United States.

In 2008, the EDPS, in coordination with other data protection authorities, intends to further encourage and closely monitor progress in this area.

## 2.6. Inspection policy

### 2.6.1. 'Spring 2007 and beyond'

According to Article 41(2) of Regulation (EC) No 45/2001, the EDPS is responsible for monitoring and ensuring the application of the regulation. In March 2007, the EDPS launched a procedure to measure compliance with the regulation in the various institutions and agencies and to maintain the effect of 'spring 2007' (see paragraph 2.3).

The first part of the operation launched in 2007 took the form of letters addressed to directors of all institutions and agencies in order to take stock of the progress made so far in various parts of the EU administration.

When proceeding to make requests, the EDPS adopted a progressive approach according to the date of creation of the agency or institution.

The first step for a series of agencies was to invite the directors to appoint a DPO. Indeed, in March 2007, 10 operational agencies had not yet appointed a DPO. Copies of the letters were sent to the responsible Commission DGs to underline the necessity to provide the DPO with adequate resources to be able to perform his/her duties.

As a result of these letters, all operational agencies have since then appointed a DPO, although in one agency this appointment is only provisional. Further-

more, in November 2007, the EDPS was informed of the appointment of a DPO at the European Investment Fund, a function which had been previously performed by the DPO of the European Investment Bank.

For those institutions and agencies where a DPO was already in office, letters were sent in April 2007 in which four groups of questions were raised, namely concerning:

- (1) the status of the DPO;
- (2) an inventory of processing operations involving personal data;
- (3) an inventory of those processing operations which fall under the scope of Article 27 of Regulation (EC) No 45/2001;
- (4) further implementation of the regulation.

A special note was sent to the Head of Administration of the EDPS, as an institution also subject to Regulation (EC) No 45/2001, requesting information on the inventory of processing operations, the inventory of processing operations subject to prior checking, and further implementation measures.

### 2.6.2. Data protection officers (DPOs)

#### Appointment of a DPO

As mentioned above, all Community institutions and agencies have appointed a DPO. The bigger institutions have also appointed an assistant DPO (European Commission, European Parliament, Council of the European Union, Court of Justice). In most cases, the assistant works on a full-time basis. Some institutions have also appointed data protection coordinators or contact persons.

#### Independence of the DPO

In his position paper on DPOs<sup>(19)</sup>, the EDPS underlined that certain elements could compromise the independent status of the DPO within institutions/agencies, namely the fact that they are part time (and that, therefore, there is a possible conflict in the allocation of time allocated to DPO work) and the hierarchi-

cal position of the DPO and the person he/she should report to.

The larger institutions (Commission, Parliament and Council) have a full-time DPO. OHIM provisionally appointed a DPO on a full-time basis from February to December 2007 so as to be able to concentrate on DPO issues. All the other institutions/agencies have a part-time DPO with no clear-cut time allocated for DPO tasks. In most of these cases, the DPO is also legal adviser.

The EDPS also underlined that independence is an issue related to the hierarchical position of the DPO and the person he/she must report to. Guarantees in this field have been provided by most institutions and agencies in the fact that the DPO function is attached to the secretary-general or director or that appraisal of the work of the DPO is submitted to the EDPS for prior consultation.

#### Adequate staff and resources

The EDPS has underlined the need for adequate staff and resources for the DPO to carry out his/her duties (IT, human resources, training, financial resources).

Most of the institutions and agencies have provided relevant information on the resources and staff provided to the DPO to enable him/her to carry out his/her duties. In some cases, assistant DPOs have been appointed. In some other cases, the DPO benefits from the assistance of other services, such as the legal service.

As for budgetary matters, only one institution has mentioned an allocated budget for the DPO. Some institutions, however, underline that they have never refused a budgetary commitment.

Some institutions/agencies mention training for the DPO mostly in the form of participation in the DPO meetings or participation in training sessions organised by the EDPS. A number of institutions/agencies have pointed out that they had set up a dedicated IT system for data protection.

### 2.6.3. Inventory of processing operations

Although not a legal obligation, the inventory of all processing operations carried out in an agency or an

---

<sup>(19)</sup> See EDPS position paper 'Role of data protection officers (DPO) in ensuring effective compliance with Regulation (EC) No 45/2001' (available on the EDPS website under the 'Consultation' section).

institution has been seen by the EDPS as a useful tool to measure compliance with the regulation. The EDPS therefore invited institutions and agencies to set up such an inventory and to report on its status to the EDPS. The EDPS also requested information on the obligation to notify the processing operations to the DPO.

Most of the agencies and institutions have established — or are establishing — such an inventory enabling them to measure compliance with the regulation.

#### 2.6.4. Inventory of prior checking cases

In his letter, the EDPS requested an overview of the state of compliance in the field of prior checking. The EDPS requested a recent inventory of all operations subject to prior checking and a status of these cases, and requested an update on the status of the cases falling in the initial priority areas (medical files, staff appraisal, disciplinary procedures, social services and e-monitoring).

Most institutions and agencies have established such an inventory enabling the EDPS to measure compliance with Article 27 of the regulation. The launching of the ‘spring 2007’ operation has led to a huge increase in the notifications of *ex post* prior checks as mentioned above (see paragraph 2.3.4). In some cases, it has indeed led to the notification of all *ex post* cases in the institution. The operation was also a good occasion for the institutions and agencies to update and inform the EDPS about the status of some pending cases and processing operations in priority areas.

#### 2.6.5. Further implementation

The EDPS also requested feedback from Community institutions and agencies on the further implementation of the regulation, including the adoption of implementing rules, and raising awareness of data protection among staff members. He requested the institutions and agencies to send models of privacy statements that they are using and asked for feedback on the general practice as to how data subjects can exercise their rights.

Article 24(8) of the regulation provides that further implementing rules concerning the DPO shall be adopted by each institution and body. They shall in particular concern the tasks, duties and powers of the DPO.

Only eight institutions/agencies have adopted implementing rules so far. Four institutions/agencies are planning to adopt these rules in 2008 and two agencies are planning to start working on them. This leaves a number of institutions/agencies without any such rules.

In order to raise awareness, information on data protection is usually given through intranet and Internet websites, publication of an electronic register, information brochures or newsletters. Some institutions have also been actively organising training or coaching of staff members or inviting external lecturers to promote data protection within the institution.

Different privacy statements have been drafted by institutions and agencies providing information contained in Articles 11 and 12 of the regulation. Most typical practices include publishing a privacy statement on the intranet or Internet, providing information on personalised staff notes, putting privacy notices on the wall where people come and go, or including data protection requirements in other documents (e.g. contracts).

As to the means by which data subjects can exercise their rights, these typically include the possibility of contacting the DPO or the controller or sending a message to a generic mailbox to that effect. Some DPOs also developed electronic forms available on their institution’s/agency’s intranet.

#### 2.6.6. Conclusions

The ‘spring 2007’ exercise has enabled the EDPS to take stock of the level of compliance of institutions and agencies with Regulation (EC) No 45/2001. A general report has been drafted to that effect by the EDPS. It has obliged agencies which had not yet done so to appoint a DPO and to consider resources and staff necessary for the performance of his/her duties. The operation has also encouraged institutions/agencies to identify processing operations containing personal data and to determine which operations are subject to prior checking by the EDPS. The operation gave impetus to the institutions and agencies to catch up on the backlog of *ex post* prior checking cases leading to a huge increase of the cases submitted to the EDPS for prior checking in 2007.

The operation must be seen as the start of an ongoing exercise by the EDPS to ensure compliance with the regulation, leading to possible on-the-spot inspections

and regular requests from the EDPS to the directors of institutions and agencies in order to assess further progress made in this field.

## 2.7. Administrative measures

Under Article 28(1), the regulation provides for the 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 DPOs (Article 24(8)).

Within the framework of consultations on administrative measures envisaged by the Community institutions or bodies, various challenging issues were raised. These issues covered the setting-up of conservation periods for certain categories of files, Internet policy papers, investigation procedures against fraud and corruption, exchange of information, implementing rules concerning data protection, and applicability of national data protection law.

### Conservation periods for certain categories of files

The EDPS was consulted by the European Commission regarding a draft common conservation list (CCL). The purpose of the CCL is to set conservation periods for the disposal of documents to be applied by the DGs/departments to certain categories of files taking into account the file administrative usefulness, as well as legal obligations.

The EDPS welcomed the fact that reference has been made to his opinions on notifications for prior checking in the area of selection, internal inquiries and social and financial aids, as well as regarding the conservation period for disciplinary files (case 2007-222).

However, the EDPS asked, *inter alia*, the justification for:

- keeping files containing administrative and financial data on the organisation of information conferences;
- keeping files implementing human resources policies for 10 years when such files contain personal data; and

- keeping personal files for up to eight years after the extinction of all rights of the person concerned and of his dependants until at least 120 years after his date of birth.

### Investigation procedures

OLAF submitted to the EDPS the short version of the revised OLAF manual concerning OLAF's statutory and procedural principles, its investigation procedures and the individual rights and information duties. The EDPS made reference to his opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations (case 2005-418). It was recommended that a future version of the OLAF manual should mention that the general rule of access to a data subject's personal data contained in the file is applied unless this access is harmful to the investigation, and any such exception is decided on a case-by-case basis and never applied systematically. The EDPS asked to be consulted before the new longer version of the OLAF manual is adopted (case 2007-310).

The EDPS issued his opinion on a draft decision by the Court of Justice modifying a previous one regarding the conditions of internal investigations concerning the fight against fraud, corruption and all illegal activities which might be prejudiced to the interests of the Communities. The EDPS made reference to his opinion on OLAF internal investigations (case 2005-418) and underlined that the guarantees provided to the data subjects were in conformity with the EDPS' guidelines in his opinion. Nevertheless, an explicit indication of the obligation of confidentiality regarding the informer's identity, as well as of Articles 11 and 12 of Regulation (EC) No 45/2001 was recommended (case 2007-167).

### Exchange of information between OLAF and Eurojust

OLAF submitted a draft accord to the EDPS on cooperation arrangements between OLAF and Eurojust, which mostly defines the *modus operandi* for the exchange of information between the two bodies, including personal data and, in some cases, also highlighting or specifying certain elements of the existing legal framework. Apart from some redrafting clarifications suggested by the EDPS, it was pointed out that OLAF should provide for the right of data subjects to be informed about the transfer of data to Eurojust or



about potential onward transfers. It has been pointed out that such a right may exist under Article 11(1)(c) and 12(1)(c) of Regulation (EC) No 45/2001, unless an exception applies (case 2007-258).

### **Internet policy papers**

The EDPS was also consulted by the DPO of the European Court of Auditors on the institution's Internet policy paper. The EDPS underlined that taking into account, on the one hand, that the monitoring of the use of the Internet as described in the Internet security policy leads to the evaluation of users' conduct and, on the other hand, that such monitoring entails the collection of data relating to suspected offences, such monitoring was, in principle, likely to be subject to prior checking under Article 27(a) and (b) of the regulation. One of the many substantive recommendations given by the EDPS was to fix a time period during which log files will be kept in order to perform monitoring and to communicate this deadline to users in the Internet security policy (case 2007-593).

The EDPS welcomed the initiative of the European Parliament's DPO concerning the 'Protocol for good practice in investigations of suspected abuses of use of Internet access or e-mail'. The EDPS found that the e-monitoring element of investigating suspected abuse of Internet or e-mail was a new element and therefore recommended that the protocol be submitted for a prior checking by the EDPS under Article 27 of the regulation. One of the EDPS' remarks concerned the need for a certain degree of seriousness of the abuse, to avoid undue investigations. Moreover, for information purposes, a reference to Article 20 of the regulation (conditions under which the obligation to inform can be deferred) was recommended. It was also important to clarify in the protocol the nature of the investigations conducted at the request of the person concerned. In addition, the EDPS underlined that the same data protection guarantees applied to administrative investigations in general (case 2007-261).

### **Implementing rules on data protection**

The EDPS provided comments on the draft implementing rules concerning data protection at the Community Fisheries Control Agency (CFCA). Apart from a series of substantive modifications, the EDPS welcomed the CFCA approach not to limit the imple-

menting rules to the DPO, as foreseen in Article 24(8) of the regulation, but to develop them to cover also the role of controllers and the rights of data subjects (case 2007-651).

A decision of the executive director adopting implementing rules concerning data protection at the European Maritime Safety Agency (EMSA) was also submitted to the EDPS. The EDPS recommended, inter alia, a description of tasks, duties and powers of the DPO, a particular reference to handle queries and complaints, and reference to Articles 11 and 12 of the regulation (case 2007-395).

In addition, the DPO of EMSA sought advice on a project regarding data protection rules on the intranet. The EDPS recommended some drafting changes for the sake of consistency with the regulation (case 2007-397).

### **Registration of national case-law on *Portail externe***

The EDPS was consulted on a draft opinion of the Court of Justice's DPO regarding the registration of national case-law on the *Portail externe* which raises questions on preliminary ruling in the field of Community law.

The EDPS pointed out that, before the publication of national case-law on the *Portail externe*, it was important to determine the necessity of the operation in the light of the purpose to be carried out. The EDPS recommended the Court of Justice to consider a methodology to anonymise the national court decisions, bearing in mind the level of transparency sought. Where the data are not made anonymous, Article 5(a) and (d) as well as Article 12 of the regulation should be taken into consideration (case 2007-444).

### **Applicability of national data protection law**

The DPO of the European Foundation for the Improvement of Living and Working Conditions (Eurofound) submitted a consultation regarding the employee data protection policy in the agency. The issue of the applicability of Irish law was raised as the agency is based in Ireland. It was pointed out that, although the case-law recognises that the immunity of Community institutions and bodies is not absolute and that national law may apply when EU law does

not cover a particular area and when no specific rules apply, the EDPS could see no justification for the reference to national data protection law. Other recommendations were made, such as on retention periods of medical, disciplinary and traffic data, as well as data relating to the monitoring of the exchange server, security or traffic management (case 2007-305).

### Other issues

The setting-up of a network of data protection correspondents within the European Parliament, as a matter of internal organisation, was also subject to consultation. The EDPS welcomed the idea of the Parliament's DPO and pointed out that such a network proved to be very positive in the European Commission in promoting and monitoring the processing of personal data, and helping data controllers to carry out their work (case 2007- 297).

The DPO of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) sought advice concerning the decisions on the compensation for work or missions performed during Saturdays, Sundays and public holidays, or between 22.00 and 7.00 and on holiday flexibility arrangements. In this case, as personal data were collected in the framework of these two procedures, the EDPS pointed out that the regulation applied. These decisions did not in themselves raise any specific data protection concerns (case 2007-725).

## 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 Regulation (EC) No 45/2001. The EDPS is developing policies 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 order to collect their comments and reactions.

These comments and reactions were taken on board and are being incorporated in a final document which also takes into account recent developments in this



The monitoring of electronic communications must respect data protection principles.

area, such as the European Court of Human Rights' decision concluding that monitoring an employee's Internet use breaches human rights<sup>(20)</sup>. The modification of Article 49 of the EC financial regulation's implementing rules relating to information on transfers for audit purposes and conservation of data will also be taken into account in the final document.

Issues in this field have also arisen in the context of other EDPS activities and are discussed elsewhere in this report (see paragraph 2.3.4 'Main issues in *ex post* cases', section on e-monitoring, and paragraph 2.7 as to consultations on Internet policy papers)

## 2.9. Video-surveillance

In 2007, the EDPS continued to work on his video-surveillance guidelines to provide practical guidance to EU institutions and bodies on compliance with data protection rules when using video-surveillance systems. Following a survey conducted among various Community institutions and bodies about their practices in 2006, the EDPS also carried out in spring 2007 an international survey among the EU Member States, with the assistance of the national data protection authorities (DPAs). The survey covered the data protection rules applied to video-surveillance practices throughout the EU.

<sup>(20)</sup> Case of *Copland v the United Kingdom*, Application No 62617/00.

Meanwhile, the EDPS also gained further practical experience in the area of video-surveillance ‘in-house’. He continued to work with the European Parliament on a follow-up to a 2006 complaint against the Parliament’s video-surveillance practices.

He also advised on three consultation requests related to video-surveillance and received from the DPOs of two institutions. All three cases involved the use of video-technology for purposes not related to security.

In the ‘info-centre’ case (2006-490), an institution installed video cameras in its info-centres (facilities allowing Internet and computer use for visitors). The footage from the info-centres, showing visitors working at their work stations, was broadcast live on the institution’s intranet, to promote the info-centre facility. An additional intended purpose was to help assisting personnel to monitor availability of space at the info-centres. In his proportionality analysis, the EDPS found that the processing was intrusive, in particular compared with the purposes it sought to achieve, and considering also the availability of other viable means to achieve those same purposes. Therefore, the EDPS recommended that the institution use other methods to promote its info-centres and monitor availability of space.

Another consultation request, the ‘loading-bay’ case (2006-510), concerned a proposed installation of cameras in loading bays at an institution’s parking lots to monitor availability of space for loading and uploading. The footage would have been available online to the procurement team. Again, the EDPS recommended (i) the use of other methods to monitor availability of space, or, alternatively, (ii) positioning of cameras or setting their resolution in such a way that no persons caught on the cameras could be identifiable.

A third case (‘video-facilities in conference rooms’) (2007-132) focused on the modalities in which notice and consent should be given when the speakers and/or participants are filmed during conferences and

other special events organised at the premises of the institution.

During 2007, the EDPS also received a number of prior checking notifications from Community institutions and bodies. With the exception of OLAF’s planned closed-circuit television (CCTV) practices, all other prior checking notifications concerned *ex post* cases.

The Commission, the JRC in Ispra, the Council, as well as the CoR, jointly with the EESC, have each submitted such an *ex post* prior checking notification to the EDPS. These cases were suspended, pending the adoption of the EDPS video-surveillance guidelines. However, OLAF’s CCTV practices, being subject to a true prior checking procedure, are currently being reviewed by the EDPS (case 2007-634).

Building on the results of the two surveys, as well as on his own experience so far, the EDPS started to prepare the first consultation draft of his video-surveillance guidelines at the end of 2007. This first consultation draft is planned to be finalised and published on the EDPS website in 2008, inviting comments from all interested parties. The EDPS plans to adopt his final guidelines after assessment of the comments received and the resulting further clarification and improvement of the guidelines. The guidelines will focus on issues relevant to the practices of the European institutions and bodies but will also take inspiration from national data protection laws, regulations and guidelines in EU Member States.



Data protection safeguards are needed to ensure the safe use of video-surveillance.



The guidelines will provide clear and detailed advice to smaller institutions or bodies with relatively simple video-surveillance systems with minimal intrusion to privacy, and thus, in many cases, will alleviate the need for controllers to subject their processing operations to the EDPS for prior checking.

However, certain more complex, novel or intrusive systems, in particular the so-called high-tech video-surveillance systems, will remain subject to prior checking by the EDPS. Approval will only be granted on a case-by-case basis. A prior checking, in some cases in an abbreviated form, will also be required for systems where the controller, due to the specific circumstances of the case, wishes to deviate from one or more of the standard recommendations set forth in the EDPS video-surveillance guidelines.

## 2.10. 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. Eurodac was set up under specific rules at the European level, including data protection safeguards <sup>(21)</sup>.

The EDPS supervises the processing of personal data in the central database, operated by a Central Unit in the Commission, and their transmission to the Member States. Data protection authorities in the Member States supervise the processing of data by the national authorities, as well as the transmission of these data to the Central Unit. In order to ensure a coordinated approach, the EDPS and national authorities meet regularly to discuss common problems relating to the functioning of Eurodac, as well as to recommend common solutions. This approach of 'coordinated supervision' has so far been very effective (see paragraph 4.3 below).

In 2005, the EDPS carried out an inspection of security and data protection measures at the Central Unit.

---

<sup>(21)</sup> Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, p. 1.

In his report, issued in February 2006, the EDPS made a series of recommendations with the aim of improving the system.

As a second step, an in-depth security audit was launched, which started in September 2006. It assessed whether the implemented security measures comply with the requirements defined by the applicable rules and the corresponding security policy of the European Commission. It further assessed whether these security measures still comply with best current practices. The final report of the audit was presented in November 2007.

According to an agreement between the EDPS and the European Network and Information Security Agency (ENISA), the agency provided contacts with national expert organisations, and delivered advice on the methodology of the security audit. The audit team was composed of representatives from the EDPS, the German Federal Office for Information Security (BSI) and the DCSSI (Direction centrale de la sécurité des systèmes d'information) from France. ENISA reviewed the quality standards of the report. While the report is EU restricted, a short summary was made available on the EDPS website <sup>(22)</sup>.

The EDPS endorsed the conclusions and recommendations. The main conclusion was that security measures initially implemented with respect to Eurodac and the way in which they have been maintained during the first four years of activity have provided a fair level of protection to date. However, some parts of the systems and the organisational security present some weaknesses which will have to be addressed in order for Eurodac to fully comply with best practices and the implementation of best available techniques.

The EDPS will review the implementation of the follow-up measures, which will be elaborated on the basis of the report. He expects that this report will also be taken into account in VIS, SIS II and other forthcoming large-scale EU systems.

---

<sup>(22)</sup> See the 'Supervision' section, under Eurodac.

## 3. Consultation

### 3.1. Introduction

In 2007, the EDPS gave further effect to his task as an advisor on proposals for EU legislation and other related documents. This task has formally been laid down in Articles 28(2) and 41 of Regulation (EC) No 45/2001.

As was the case in previous years, the EDPS consultative activities essentially focused on the impact of proposals for legislation in different policy areas on the level of data protection. This consultative role is guaranteed under the general legal framework for data protection under the EC Treaty (mainly the data protection Directive 95/46/EC) as well as according to the general principles for data protection applicable under Title VI of the EU Treaty (the so-called 'third pillar', a significant area of intervention for the EDPS).

However, more than in previous years, the future of the legal framework for data protection itself was the subject of activities of the EDPS. In the first place, 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<sup>(23)</sup> continued to require much attention from the EDPS. In the second place, in his opinion<sup>(24)</sup> on the Commission communication on the implementation of the data protection directive<sup>(25)</sup>, the EDPS expressed

<sup>(23)</sup> Proposal for a Council framework decision, of 4 October 2005, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final).

<sup>(24)</sup> Opinion of 25 July 2007 on the communication from the Commission to the European Parliament and the Council on the follow-up of the work programme for better implementation of the data protection directive (OJ C 255, 27.10.2007, p. 1).

<sup>(25)</sup> Communication from the Commission to the European Parliament and the Council, of 7 March 2007, on the follow-up of the work programme for better implementation of the data protection directive (COM(2007) 87 final).

the view that changes to the directive seem unavoidable in the longer term and suggested that thought be given to future changes as early as possible. In the third place, the Lisbon Treaty was signed with considerable implications for data protection. Before the treaty was finalised, the EDPS brought a few specific points to the attention of the Portuguese Presidency for consideration.

Moreover, the EDPS considered for the first time the need for a specific legal framework for data protection in a specific area (the use of radio frequency identification (RFID) technology) should the proper implementation of the existing general legal framework fail. This specific area is essentially new and may have an important impact on our society and on the protection of fundamental rights such as privacy and data protection.

Two other points need to be highlighted for 2007.

- For the first time, the EDPS concluded that a legal instrument, as proposed by the Commission, should not be adopted; this conclusion was drawn up in his opinion on the proposal for a Council framework decision on the use of passenger name record (PNR) data for law enforcement purposes<sup>(26)</sup>.
- For the first time, the EDPS presented an opinion on a Commission communication — actually on two occasions (see paragraph 3.3.2).

The activities of the EDPS took place in the context of different developments having as common denominator the fact that they all contribute to the emerging

<sup>(26)</sup> Opinion of 20 December 2007 on the proposal for a Council framework decision on the use of passenger name record (PNR) data for law enforcement purposes.



Part of the consultation team discussing a legislative opinion.

of a 'surveillance society'. These developments are described below.

- In the area of freedom, security and justice, major trends continue. Again, new instruments to widen the possibilities for law enforcement authorities to collect, store and exchange personal data have been proposed, in particular for the fight against terrorism and organised crime.
- The impact of technology on privacy and data protection becomes more and more visible. The increased use of biometrics and development of RFID required specific attention.
- The growing importance of international data flows cannot always be traced and in any event are not fully covered by EU data protection laws, given the limitations of their territorial scope.

As to the working methods of the EDPS, 2007 was the first year for which the EDPS' working priorities were laid down in a public document, namely the 'Inventory 2007', which was published on the EDPS website in December 2006.

The output in terms of number of opinions issued shows the smallest possible increase, as compared with 2006: 12 opinions have been issued in 2007; 11 in 2006. The EDPS has made more use of other instruments of intervention, such as comments (which are also published on the website, but not in the *Official Journal of the European Union*). This choice of instrument must not be seen as a structural shift in approach.

Finally, this chapter will not only look back at the activities over 2007, but will also look ahead by describing new developments in technology, as well as in legislation.

### 3.2. Policy framework and priorities

The policy paper entitled 'The EDPS as an advisor to the Community institutions on proposals for legislation and related documents' <sup>(27)</sup> can be considered as setting out the main lines along which the EDPS operates

in the area of consultation.

The paper includes three elements: the scope of the advisory task of the EDPS, the substance of the interventions, and the approach/working methods. This policy paper was issued in March 2005 and has proved to be a solid basis for the activities of the EDPS.

This basis was further elaborated and refined in 2007. The EDPS has clarified that the objective of his participation in the EU legislative process is to actively promote that legislative measures will only be taken after due consideration of the impact of the measures on privacy and data protection. The impact assessments conducted by the Commission must give appropriate attention to privacy and data protection. In addition, decisions must always be based on awareness of the impact on data protection.

Furthermore, a research assistant within the EDPS has started the preparation of a report on the common lines and principles developed by the EDPS in his consultative activities, within the area of freedom, security and justice. This report must be seen as a further step in promoting a consistent approach, and as an essential element of effectiveness. At this stage, the EDPS has opted for a fairly limited scope — the area of freedom, security and justice — but in the longer term a similar initiative could be considered for the

<sup>(27)</sup> Available on the EDPS website under the 'Consultation' section.

whole area of activity of the EDPS. The report will be completed in early 2008.

As regards the approach and working methods, 2007 proved to be a year of consolidation. Consultation of the EDPS — which includes activities at different stages in the legislative procedure — has become a normal part of this procedure, provided of course that proposals have or may have an impact on data protection.

### The inventory

The yearly inventory must be seen as an additional part of the policy framework of the EDPS. The inventory consists of two parts:

- an introduction providing a short analysis of the context and a specification of the priorities over the considered year;
- an annex which lists the relevant Commission proposals (and related documents) that may require a reaction from the EDPS; the main source of the annex is the Commission legislative and work programme.

The Inventory 2007 listed eight priorities for the EDPS. Generally speaking, the EDPS has performed along the lines of these priorities. Taking a closer look at the different priorities, the following conclusions can be drawn.

The annex of the Inventory 2007 listed 16 important documents (mentioned as ‘red’) on which the EDPS intended to issue an opinion. This purpose has led to the following result:

| Opinion issued                               | 8 documents                   |
|--|-------------------------------|
| No EDPS opinion but support to opinion WP 29 | 1 document (PNR-US agreement) |
| EDPS opinions postponed to 2008              | 2 documents                   |
| Commission proposal postponed to 2008        | 5 documents                   |

Furthermore, the list contained 22 documents of less importance to the EDPS, on which the EDPS intended to possibly issue an opinion, to react in another way or to just closely follow policy developments in the area.

**Priority 1:** The storage and exchange of information in the area of freedom, security and justice has again been a core activity of the EDPS in 2007 (and will remain so as long as the EU legislator continues to put emphasis on new legal instruments or modification of existing instruments in this area).

**Priority 2:** The communication of the Commission on the future of Directive 95/46/EC has led to an extensive EDPS opinion, in which he asked to start to consider future changes.

**Priority 3:** The developments taking place in the ‘information society’ have been closely followed and commented on. RFID has been mentioned; the EDPS has been involved in the modification of Directive 2002/58/EC (opinion will follow early in 2008).

**Priority 4:** As to the priority of including ‘public health’ as an essential area for the EDPS, not much progress has been made, mainly due to the fact that no relevant legislative proposals have been adopted in 2007. This subject will remain a priority in 2008.

**Priority 5:** Many activities have been employed relating to the area of OLAF. Specific attention has been given to the exchange of personal data with Europol (dealt with in the EDPS opinion on the Europol decision) and the exchange of data with third countries. There is a clear relation with the supervision of the EDPS on the processing by OLAF.

**Priority 6:** As to transparency, advisory activities have been postponed in the perspective of the judgment of the Court of First Instance in *Bavarian Lager* (delivered on 8 November 2007). A proposal for modification of Regulation (EC) No 1049/2001 is now foreseen for spring 2008.

**Priority 7 and 8:** Horizontal themes and other activities (relating to working method): considerable progress has been made.

The state of play at the end of 2007 shows a diverse image.

|   |   |
|---|---|
| EDPS continuous attention (research programmes, general issues/subjects such as immigration or public health) | 8 documents   |
| EDPS involvement in 2007 (comments or informal action)  | 4 documents (spam, cybercrime, terrorism, public-private partnership) |
| Deleted from list without further action by EDPS  | 5 documents   |
| Commission activity postponed to 2008   | 2 documents   |
| Upgraded to 'red' issue in Inventory 2008   | 3 documents   |

### Inventory 2008

In December 2007, the Inventory 2008 (the second yearly inventory) was published on the website. It follows the main lines as set out in the Inventory 2007. The priorities are arranged in a slightly different way: the Inventory 2008 only lists **six priorities**, two of which are new. In 2008, priority will also be given to the preparation of the entry into force of the Lisbon Treaty, as well as to external aspects of data protection relating to the transfer of data to third countries.

The annex of the inventory shows that the scope of activity of the EDPS now covers a wide range of policy areas. The proposals listed relate to 13 different Commission services (Personnel and Administration DG, Employment, Social Affairs and Equal Opportunities DG, Enterprise and Industry DG, Eurostat, Information Society and Media DG, Justice, Freedom and Security DG, Internal Market and Services DG, OLAF, External Relations DG, Health and Consumer Protection DG, Secretary-General, Taxation and Customs Union DG, Energy and Transport DG).

There is also an increase of the total number of proposals listed in the annex. The annex now mentions 67 topics divided along the following lines:

- 34 topics are flagged as red, having a high priority; 33 topics are marked as 'yellow' documents, covering documents of less importance to the EDPS on which the EDPS intends to possibly react;
- 29 topics can be defined as legislative proposals *stricto sensu* (for regulations, directives, decisions

and framework decisions); the other 38 topics are non-legislative documents; this includes the Commission communications, recommendations, work programmes, as well as documents relating to agreements between the EU and third countries.

This increase in the number of proposals listed in the annex is partly due to the fact that the annex is based on the Commission legislative and work programme, which lists closely related topics as separate items. The fact that 34 topics have been granted a 'red' priority does not necessarily mean that the number of EDPS opinions will grow accordingly.

## 3.3. Legislative opinions

### 3.3.1. General remarks

#### Opinions on third pillar issues

The EDPS adopted 12 legislative opinions in 2007. As in previous years, a substantial part of the opinions relate to the area of freedom, security and justice. However, this area now represents somewhat less than 50 % of the legislative opinions (namely 5 out of 12). All five opinions concerned documents in the field of police and judicial cooperation in criminal matters (the third pillar) and included fundamental developments, not least from the perspective of data protection. This is so in the first place with the third opinion 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. The other opinions deal with the proposal for a Europol decision, the two initiatives on cross-border cooperation (transposing the Prüm Treaty and its implementing agreement to the EU level) and the proposal for a European passenger name record (PNR) system.

In the third pillar, a major concern was the adoption of new proposals facilitating the storage by and exchange of information between law enforcement authorities, without a proper assessment of the effectiveness of existing legal instruments. New instruments are designed before existing instruments have been properly implemented. This problem was of particular relevance in relation to the transposition of the Prüm Treaty to the EU level and to the European PNR system.



Another problem that played a central role in the opinions of the EDPS relating to third pillar issues was the lack of a comprehensive legal framework for data protection. Most proposals include some specific provisions on data protection aiming at setting up a general framework. However, a satisfactory legal framework has not yet been put in place.

A third issue at stake is the fact that EU rules make it mandatory for Member States to establish national authorities for certain tasks, but leave them with a wide discretion in the conditions for the functioning of these authorities. This hampers the exchange of information between the Member States and affects the legal certainty of the data subject whose data are transferred between the authorities of different Member States.

The exchange of information with third countries for law enforcement purposes was a separate issue, discussed in different EDPS opinions. The EDPS was concerned about the lack of harmonisation, as well as the lack of guarantees surrounding the processing by third countries, following the transfer of the personal data.

### Opinions on communications

Two opinions were issued with regard to important Commission communications relating to the future framework for data protection. In his opinion on the implementation of the data protection directive<sup>(28)</sup>, the EDPS identified five perspectives of a changing context, one of which being the interaction with technology. New technological developments have a clear impact on the requirements for an effective legal framework for data protection. An important technological development is RFID, the subject of a separate EDPS opinion<sup>(29)</sup>.

The two opinions released on Commission communications gave the EDPS the opportunity to reflect on future perspectives for data protection and to give an impetus to discussions on the data protection framework in the near future; such discussions are needed and becoming urgent (see paragraph 3.7 on future developments).

<sup>(28)</sup> Opinion of 25 July 2007 on the communication from the Commission to the European Parliament and the Council on the follow-up of the work programme for better implementation of the data protection directive, OJ C 255, 27.10.2007, p. 1.

<sup>(29)</sup> Opinion of 20 December 2007 on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on radio frequency identification (RFID) in Europe: steps towards a policy framework (COM(2007) 96).

### Opinions on first pillar legislation

The other five opinions released by the EDPS in 2007 were of a varied nature and dealt with policy areas such as customs, statistics, road transport, agriculture and social security. The main common denominator is that three out of five opinions discuss proposals that facilitate the exchange of data between Member States' authorities (on customs, road transport and social security). Other issues covered include the disclosure of information on beneficiaries of Community funding, the concept of statistical confidentiality, and the relation between specific rules and the general data protection framework.

The proposals reflect a more general trend. Information exchange between Member States — including exchange of personal data — is seen as an important instrument in the development of the internal market. Barriers could be taken away by facilitating the exchange, by fully using the possibilities of electronic networks. Sometimes a role is foreseen for the Commission as responsible for the maintenance and availability of the technical infrastructure. In those cases, the EDPS also acts as a supervisory authority.

In general, this trend requires close attention from the EDPS, to ensure that the necessary safeguards and guarantees for the data subject are taken into account, as part of the instruments facilitating the exchange of personal data. In this respect, it is also essential that a data subject can exercise his or her rights in a simple and practical way.

### 3.3.2. Individual opinions

#### European Police Office (Europol)

In 1995, Europol was created on the basis of a convention between the Member States. This convention has a disadvantage in terms of flexibility and effectiveness as all modifications must be ratified by all the Member States, a process which may take years as demonstrated by experiences in the past.

The objective of the proposal for a Council decision replacing the convention<sup>(30)</sup>, on which the EDPS

<sup>(30)</sup> Proposal for a Council decision, of 20 December 2006, establishing the European Police Office (Europol) (COM(2006) 817 final).

issued an opinion on 16 February 2007<sup>(31)</sup>, is not a major change in the mandate or the activities of Europol, but mainly consists in providing Europol with a new and more flexible legal basis. The proposal also contains substantive changes, so as to further improve Europol's functioning. It extends the mandate of Europol and lays down several new provisions, aiming to further facilitate the work of Europol, for instance regarding the exchange of data between Europol and other bodies of the EC/EU, such as OLAF. The proposal also contains specific rules on data protection and data security, additional to the general legal framework on data protection for the third pillar that has not yet been adopted.

The EDPS opinion concludes that the Council decision should not be adopted before the adoption of a framework on data protection that will ensure an appropriate level of data protection.

Moreover, suggestions are made for improvements such as:

- ensuring that data collected from commercial activities are accurate;
- applying strict conditions and guarantees when databases are interlinked;
- harmonising rules on, and limiting the exceptions to, the data subject's right of access;
- including guarantees for the independence of Europol's data protection officer (who internally ensures lawful processing of personal data);
- ensuring supervision of the EDPS on data processing concerning staff of Europol.

#### **Correct application of the law on customs and agricultural matters**

On 22 February 2007, the EDPS advised on a Commission proposal for a regulation which foresees the creation or updating of various IT systems containing personal data. The aim of the proposal is to strengthen the cooperation between Member States and the Commission to avoid breaches to customs and agricultural legislation<sup>(32)</sup>. The IT systems include the

European data directory, the customs information system (CIS) and the customs files identification database (FIDE).

In his opinion<sup>(33)</sup>, the EDPS suggests various amendments to the proposal in order to ensure the proposal's overall compatibility with the existing legal framework on data protection and the effective protection of individuals' personal data. Among others, the EDPS suggested the following:

- the Commission should carry out a proper assessment regarding the need to create the European data directory;
- if the European data directory is created, the regulation should provide for the adoption of complementary administrative rules setting forth specific measures to ensure the confidentiality of the information;
- to amend various provisions in order to recognise the EDPS supervisory role regarding CIS and FIDE;
- to create a coordinated approach for the supervision of CIS which would include the national authorities and the EDPS.

#### **Coordination of social security systems**

On 6 March 2007, the EDPS advised on a Commission proposal containing implementing measures on coordination of social security systems. The proposal covers a vast range of areas in social security (pensions, benefits in respect of maternity, invalidity, unemployment, etc.)<sup>(34)</sup>. It aims at modernising and simplifying the existing rules by strengthening cooperation and improving methods of data exchange between social security institutions of the different Member States.

The EDPS welcomed the proposal to the extent that it aims at favouring the free movement of citizens and improving the standard of living and conditions of employment of those moving within the Union<sup>(35)</sup>.

<sup>(31)</sup> Opinion of 16 February 2007 on the proposal for a Council decision establishing the European Police Office (Europol) (COM(2006) 817 final), OJ C 255, 27.10.2007, p. 13.

<sup>(32)</sup> Proposal for a regulation of the European Parliament and of the Council, of 22 December 2006, amending Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (COM(2006) 866 final).

<sup>(33)</sup> Opinion of 22 February 2007 on the proposal for a regulation amending Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (COM(2006) 866 final), OJ C 94, 28.4.2007, p. 3.

<sup>(34)</sup> Proposal for a regulation of the European Parliament and of the Council, of 31 January 2006, laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems (COM(2006) 16 final).

<sup>(35)</sup> Opinion of 6 March 2007 on the proposal for a regulation laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems (COM(2006) 16 final), OJ C 91, 26.4.2007, p. 15.

While it is true that social security could not exist without the exchange of different kinds of personal data, it is also true that a high level of protection of these data is necessary. Bearing this in mind, the EDPS advised to:

- pay the utmost attention to basic data protection principles such as purpose limitation as well as proportionality in data processed, bodies authorised to process data and retention periods;
- ensure that each proposed mechanism for the storage and transmission of personal data is clearly based on specific legal grounds;
- provide the concerned persons with relevant information on the processing of their personal data;
- enable data subjects to exercise their rights effectively in a trans-border context.

#### Cross-border cooperation (Prüm Treaty)

On 4 April 2007, the EDPS presented an opinion on the initiative of 15 Member States to make the Treaty of Prüm applicable throughout the EU, although he had not been consulted on this proposal <sup>(36)</sup>.

The initiative aims to step up cross-border cooperation, particularly for combating terrorism and cross-border crime. The initiative deals with the exchange of biometric data (DNA and fingerprints) and requires Member States to set up DNA databases <sup>(37)</sup>.

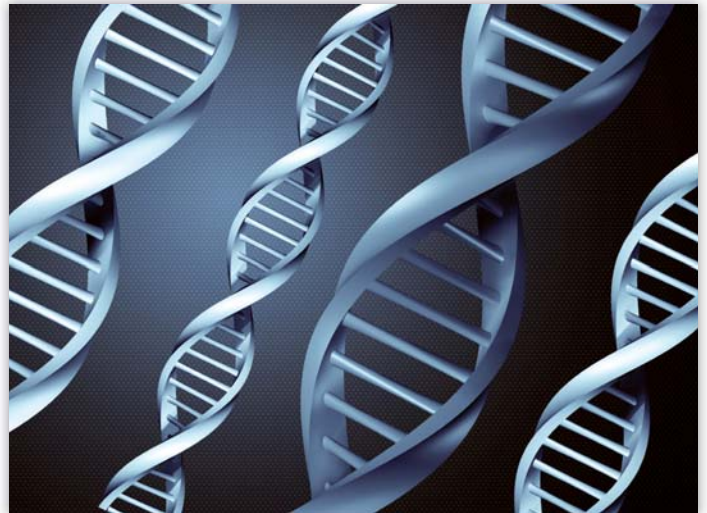
Although data protection plays an important role in this initiative, the provisions are meant as specific ones — on top of a general framework for data protection, which has still not been adopted. Such a framework is needed to give citizens enough protection, since this decision will make it much easier to exchange DNA and fingerprint data.

Since the Prüm Treaty has already entered into force in some Member States, the EDPS' suggestions mainly serve to improve the text without modifying the system of information exchange itself. In particular, he notes that:

- the approach relating to the different kinds of personal data is good: the more sensitive the data, the more limited the purposes for which they can be used and the more limited the access is;

<sup>(36)</sup> Opinion of 4 April 2007 on the initiative of 15 Member States with a view to adopting a Council decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ C 169, 21.7.2007, p. 2.

<sup>(37)</sup> Prüm initiative, OJ C 71, 28.3.2007, p. 35.



The Prüm decision relies on making use of DNA material.

- the Council should include an impact assessment and an evaluation clause in the procedure of adoption; he warned that a system elaborated for a small number of closely cooperating Member States is not automatically appropriate to be used on an EU-wide scale;
- the initiative does not specify the categories of persons that will be included in the DNA databases and it does not limit the retention period.

#### Financing of the common agricultural policy

The analysed proposal aims at fulfilling the requirement for the publication of information on beneficiaries of Community funds. In order to implement the European transparency initiative, Council Regulation (EC, Euratom) No 1995/2006 of 13 December 2006 <sup>(38)</sup>, which was also the subject of an opinion of the EDPS, inserted this requirement into the financial regulation.

The main aspect analysed by the EDPS in his opinion of 10 April 2007 relates to the fact that Member States should ensure annual *ex post* publication of the beneficiaries and the amount received per beneficiary under the European funds, which form part of the budget of the European Communities.

<sup>(38)</sup> Council Regulation (EC, Euratom) No 1995/2006 of 13 December 2006 amending Regulation (EC, Euratom) No 1605/2002 on the financial regulation applicable to the general budget of the European Communities, OJ L 390, 30.12.2006, pp. 1–26.

In his opinion, the EDPS supports the inclusion of the transparency principle and underlines that a proactive approach to the rights of the data subjects should be followed. Furthermore, this proactive approach could consist of informing the data subjects beforehand, at the time the personal data are collected, that these data will be made public, and of ensuring that the data subject's right of access and right to object are respected.

Moreover, the EDPS suggests introducing a specific provision, which will help to comply with Article 12 of Regulation (EC) No 45/2001. The aim is to inform data subjects about the processing of their personal data by auditing and investigating institutions and bodies.

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

On 20 April 2007, the German Presidency consulted the European Parliament on a revised proposal for a Council framework decision<sup>(39)</sup>. The aim of the revision was to speed up negotiations in the Council and to improve data protection in the third pillar. The EDPS considered that the substantive changes contained in the revised proposal, as well as its importance, called for a new opinion, which was issued on 27 April 2007<sup>(40)</sup>. In his two previous opinions on the subject, the EDPS stressed the need for a general framework for data protection in an area of freedom, security and justice where enhanced police and judicial cooperation is acquiring growing relevance.

In this third opinion, the EDPS takes a critical position, recommending that the framework decision should not be adopted without significant improvements, in particular with regard to the following issues:

- extension of the scope to also include domestic data processing, so that citizens' data are adequately protected not only when exchanged with another Member State;
- limiting the purposes for which personal data may be further processed, to avoid contradicting the basic principles of Convention 108;

- requiring an adequate level of protection for exchanges with third countries according to a common EU standard;
- ensuring data quality, by distinguishing between factual and 'soft' data, as well as between categories of persons, such as witnesses, convicted persons, etc.

Furthermore, the EDPS advised the Council against negotiating new issues raised in the proposal — extending its scope to third pillar data processing by Europol and Eurojust, as well as establishing a new joint supervisory authority — for fear that some other essential elements of the proposal would not be sufficiently addressed.

#### **Communication on the implementation of the data protection directive**

The Commission's communication on the implementation of the data protection directive reiterates the importance of Directive 95/46/EC as a milestone in the protection of personal data and discusses the directive and its implementation<sup>(41)</sup>. The central conclusion of the communication is that the directive should not be amended. The implementation of the directive should be further improved by means of other policy instruments, mostly with a non-binding nature.

The opinion of the EDPS of 25 July 2007 supports the central conclusion of the Commission. According to him, in the short term, energy is best spent on improvements to the implementation of the directive<sup>(42)</sup>. In the longer term, however, changes to the directive seem unavoidable. The EDPS asks that a clear date for a review to prepare proposals leading to such changes should already be set now. Such a date would give a clear incentive to start thinking about future change. Future change does not mean a need for new principles, rather a clear need for other administrative arrangements.

The opinion singles out five perspectives for future change: full implementation of the directive, interaction

---

<sup>(39)</sup> Council Document 7315/07 of 13 March 2007.

<sup>(40)</sup> Third opinion of 27 April 2007 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, OJ C 139, 23.6.2007, p. 1.

<sup>(41)</sup> Communication from the Commission of 7 March 2007 to the European Parliament and the Council on the follow-up of the work programme for better implementation of the data protection directive (COM(2007) 87 final).

<sup>(42)</sup> Opinion of 25 July 2007 on the communication from the Commission to the European Parliament and the Council on the follow-up of the work programme for better implementation of the data protection directive, OJ C 255, 27.10.2007, p. 1.

with technology, global privacy and jurisdiction, law enforcement, and the impact of the Lisbon Treaty.

As to the perspective of full implementation, the EDPS calls on the Commission to consider a series of recommendations that would include:

- in certain cases, specific legislative action at EU level;
- to pursue a better implementation of the directive through infringement procedures;
- the use of the instrument interpretative communication for the following issues: the concept of personal data, the definition of the role of data controller or data processor, the determination of applicable law, the purpose limitation principle and incompatible use, legal grounds for processing, especially with regard to unambiguous consent and balance of interests;
- the wide use of non-binding instruments including instruments building on the concept of 'privacy by design';
- the submission of a paper to the Article 29 Working Party giving clear indications on the division of roles between the Commission and the working party.

### Community statistics on health

On 5 September 2007, the EDPS adopted an opinion on the proposal for a regulation of the European Parliament and of the Council on Community statistics on public health and health and safety at work <sup>(43)</sup>.

The proposal aims at establishing the framework for all current and foreseeable activities in the field of public health and health and safety at work statistics carried out by Eurostat, national statistical institutes and all other national authorities responsible for the provision of official statistics in these areas.

The main recommendations of the EDPS referred to the necessity to address the differences between data protection and statistical confidentiality, namely to the notions which are specific to each area. Moreover, the issue of transfers of personal data to third countries as well as conservation periods of statistical data were also analysed.

<sup>(43)</sup> Opinion of 5 September 2007 on the proposal for a regulation of the European Parliament and of the Council on Community statistics on public health and health and safety at work (COM(2007) 46 final), OJ C 295, 7.12.2007, p. 1.

Following discussion between the services of Eurostat and the EDPS, it was decided that a common review of the processes put in place in Eurostat when dealing with individual records for statistical purposes would be conducted and could lead to the need for prior checking.

### Road transport operators

On 12 September 2007, the EDPS issued his opinion on the proposal for a regulation of the European Parliament and of the Council establishing common rules concerning the conditions to be complied with to pursue the occupation of road transport operator <sup>(44)</sup>.

The regulation establishes conditions relating to good repute, financial standing and professional competence which road transport companies have to satisfy. The proposal introduces national electronic registers that will have to be interconnected between all Member States, facilitating the exchange of information between Member States. It contains a specific provision on data protection <sup>(45)</sup>.

The EDPS advises that the proposed regulation is amended to:

- ensure greater definition of terms such as 'good repute';
- clarify ambiguities in the role of national authorities;
- ensure that the requirements of Directive 95/46/EC are respected.

### Implementing rules of the Prüm initiative

On 19 December 2007, the EDPS presented his opinion on the German initiative establishing implementing rules which are necessary for the functioning of the Council decision on Prüm <sup>(46)</sup> (the EDPS already issued an opinion on the initiative for this decision on 4 April 2007).

The implementing rules and their annex have a specific importance since they define crucial aspects and tools for the exchanges of data that are essential to ensure

<sup>(44)</sup> Opinion of 12 September 2007 on the proposal for a regulation establishing common rules concerning the conditions to be complied with to pursue the occupation of road transport operator, OJ C 14, 19.1.2008, p. 1.

<sup>(45)</sup> COM(2007) 263 final of 6.7.2007.

<sup>(46)</sup> Opinion of 19 December 2007 on the initiative of the Federal Republic of Germany, with a view to adopting a Council decision on the implementation of Decision 2007/.../JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.



guarantees for concerned persons. Furthermore, the current lack of a general EU framework that would guarantee harmonised data protection in the law enforcement sector calls for specific attention to these rules.

In particular, the EDPS opinion recommends that:

- the combination of general provisions and specific tailored rules on data protection should ensure both the rights of citizens and the efficiency of law enforcement authorities when the proposal enters into force;
- the accuracy in searches and comparisons of DNA profiles and fingerprints should be duly taken into account and constantly monitored, also in the light of the larger scale of the exchange;
- data protection authorities should be put in a position to properly carry out their supervisory and advisory role throughout the different stages of implementation.

### Communication on radio frequency identification (RFID)

On 20 December 2007, the EDPS issued his opinion on the Commission's communication on radio frequency identification (RFID) <sup>(47)</sup> in Europe that was released in March 2007. The opinion deals with the growing use of RFID chips in consumer products and other new applications affecting individuals.

The EDPS welcomes the Commission's communication on RFID as it addresses the main issues arising from the deployment of RFID technology while taking account of privacy and data protection considerations. The EDPS agrees with the Commission that it is appropriate in the first phase to leave room for self-regulatory instruments. However, additional legislative measures may be necessary to regulate RFID usage in relation to privacy and data protection.

The EDPS underlines that RFID systems could play a key role in the development of the European information society but that the wide acceptance of RFID technologies should be facilitated by the benefits of consistent data protection safeguards. Self-regulation alone may not be enough to meet the challenge. Legal

<sup>(47)</sup> Opinion of 20 December 2007 on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on radio frequency identification (RFID) in Europe: steps towards a policy framework (COM(2007) 96).



'Internet of things': a tagged environment will have to be a privacy friendly environment.

instruments may therefore be required to guarantee that the technical solutions to minimise the risks for data protection and privacy are in place. Indeed, the existing data protection directive is sufficient to protect privacy in a first phase. However, the current framework should be applied effectively. There is no need for changing the principles, but additional specific rules may be required to ensure adequate results.

More specifically, the EDPS calls on the Commission to consider the following recommendations:

- the provision of a clear guidance, in close cooperation with relevant stakeholders, on how to apply the current legal framework to the RFID environment;
- the adoption of Community legislation regulating the main issues of RFID usage in case the effective implementation of the existing legal framework fails;
- such measures should notably lay down the opt-in principle at the point of sale as a precise and undeniable legal obligation;
- the identification of 'best available techniques' which will play a decisive role in the early adoption of the privacy-by-design principle.

### **Council framework decision on the use of passenger name record (PNR) data for law enforcement purposes**

The proposal for a Council framework decision foresees obligations for air carriers to transmit data about all passengers on flights to or from an EU Member State, for the purpose of combating terrorism and organised crime <sup>(48)</sup>.

In his opinion of 20 December 2007 <sup>(49)</sup>, the EDPS emphasises the major impact the proposal would have on privacy and data protection rights of air passengers. While acknowledging that the fight against terrorism is a legitimate purpose, the EDPS considers that the necessity and proportionality of the proposal are not sufficiently established. In addition, the EDPS takes a critical stance on the lack of clarity in relation to various aspects of the proposal, in particular the applicable legal framework, the identity of the recipients of personal data, and the conditions of transfer of data to third countries.

The opinion focuses on four key issues and draws the following conclusions:

- legitimacy of the processing: the proposal does not provide for sufficient elements of justification to support and demonstrate the legitimacy of the processing of data;
- applicable legal framework: a significant lack of legal certainty is noted as regards the data protection regime applicable to the different actors involved in the processing of personal data;
- the identity of data recipients: the proposal does not specify the identity of the recipients of personal data, which is essential to evaluate the guarantees that these recipients will provide;
- transfer of data to third countries: it is essential that conditions of transfer of PNR data to third countries be coherent and subject to a harmonised level of protection.

Finally, the EDPS advises not to adopt the decision before the Lisbon Treaty's entry into force, so that it can follow the ordinary legislative procedure foreseen

by the new treaty and the European Parliament is fully involved.

## **3.4. Comments**

### **Security and privacy**

On 11 June 2007, the EDPS sent letters to the Portuguese Ministers for Justice and the Interior. He called on the upcoming presidency to ensure sufficient consideration of data protection implications before Council initiatives are adopted. The EDPS expressed his concern that a number of agreements on new anti-terrorist measures had been concluded without fully considering the impact on fundamental rights.

The EDPS underlined that messages such as 'no right to privacy until life and security are guaranteed' were developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford. He expressed his concern that such a negative approach to individual privacy rights reveals an apparent lack of understanding of the framework of human rights law, which has always allowed for necessary and proportionate measures to combat crime and terrorism.

This approach also ignores the lessons learned about the abuse of fundamental rights from dealing with terrorism within Europe's borders over the last 50 years. There should be no doubt that effective anti-terror measures can be framed within the boundaries of fundamental rights. In the past, examples can be found in different parts of Europe where the failure to protect fundamental rights has served as a source of continued unrest rather than to ensure safety and stability.

In effect, the EDPS wants to ensure that data protection is regarded as a condition for the legitimacy — and indeed also for the success — of any new initiative in this field, and demonstrate the benefits of effective data protection for security and law enforcement across Europe.

The EDPS finally urged the Council — just like the European Commission — to make use of his availability as an advisor on all matters concerning personal data processing. A wide range of EDPS advice to the Commission for EU instruments in the first as well as in the third pillar resulted in improved legislation both in terms of legitimacy and efficiency.

<sup>(48)</sup> Proposal for a Council framework decision of 6 November 2007 on the use of passenger name record (PNR) data for law enforcement purposes (COM(2007) 654 final).

<sup>(49)</sup> Opinion of 20 December 2007 on the proposal for a Council framework decision on the use of passenger name record (PNR) data for law enforcement purposes.

These concerns were discussed in a meeting between the EDPS and the Portuguese Minister for Justice on 17 September 2007, where the latter confirmed his commitment to proper respect for privacy and other fundamental rights in all relevant legislation.

### **Lisbon Treaty**

In a letter sent to the Intergovernmental Conference (IGC) presidency on 23 July 2007, the EDPS asked for some specific points to be included in the data protection provisions of the new treaty with a view to improving the text of the Treaty on the European Union and the Treaty on the Functioning of the European Union, as well as the 'Declaration on personal data protection in the areas of police and judicial cooperation in criminal matters'. Unfortunately, the IGC presidency did not respond to the suggestions of the EDPS.

### **Developments on data protection framework decision**

Further to his third opinion on data protection in the third pillar, the EDPS closely followed the developments in the political debate on this crucial piece of legislation. The EDPS contacted the Portuguese Presidency so as to provide advice on some essential elements of the proposal. On 16 October 2007, the EDPS also issued comments on a few important but more technical points that should not be overlooked at the stage of finalisation of the Council framework decision.

In particular, the EDPS recommended to:

- take into account the minimal level of protection provided for by Convention 108, especially with regard to processing of sensitive data;
- clarify the relations between the limitation of the purposes for which personal data are collected and the possibility for law enforcement authorities to use them in certain cases for other incompatible purposes;
- ensure a full right of access to personal data, especially in case of automatic decisions;
- guarantee the advisory role of data protection authorities, also through a forum at EU level where these authorities could coordinate their activity.

The EDPS was also invited to present his position at the European Parliament's Committee on Civil Liber-

ties, Justice and Home Affairs (LIBE). In 2008, the EDPS will keep monitoring this proposal and will remain available to provide further advice.

### **Control of the acquisition and possession of weapons**

In a letter of 31 October 2007 sent to the European Parliament's Rapporteur appointed for the issue, the EDPS reacted to the developments in the legislative procedure on the proposal for a directive regulating the control of the acquisition and possession of weapons<sup>(50)</sup>.

These developments raise an important issue of data protection, mainly as a consequence of an amendment included in the Rapporteur's report. This amendment introduces the maintenance of a computerised and centralised data-filing system in each Member State, in which several data will be stored for not less than 20 years.

In his letter, the EDPS also raised several concerns relating to the compliance of the system with Directive 95/46/EC.

### **Rome II regulation on the law applicable to non-contractual obligations**

On 28 February 2007, the EDPS sent a letter to the presidents of the Council, the Commission and the Parliament expressing some doubts and concerns on the proposed Article 7a (violations of privacy and rights relating to the personality) of the European Parliament legislative resolution on the Council common position with a view to the adoption of a regulation of the European Parliament and of the Council on the law applicable to non-contractual obligations ('Rome II').

Indeed, this article could have created certain inconsistencies with Directive 95/46/EC. In the first place, it was not completely clear whether this article was intended to cover violations of legal rules for the processing of personal data as provided for in the directive and related instruments, and if so to which extent this might have been the case. To the extent in which that new Article 7a would have applied to violations

---

<sup>(50)</sup> Letter on the proposal for a directive amending Council Directive 91/477/EEC on the control of the acquisition and possession of weapons, 31 October 2007.

of legal rules within the scope of the directive, it was noted that it took a different approach from Article 4 of the directive as to applicable law.

In the second place, there were a number of more detailed concerns as to the only part of Article 7a which explicitly mentioned the notion of 'personal data'. It was not clear whether this paragraph would have covered data processing in general or only by a broadcaster. Moreover, the text of paragraph 3 presented some terminological inconsistencies with the directive.

The EDPS suggested that a more careful approach should be taken in the upcoming legislative instances in order to arrive at a clear view of the implications that the proposed text might have in relation to existing data protection legislation, and also to avoid the potential problems that had been briefly described in the letter.

On 11 July 2007, the regulation was adopted<sup>(51)</sup>. Article 7a was deleted. A revision clause was included in Article 30.2 specifying that a study on the situation in the field of the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality should be submitted by the Commission no later than 31 December 2008.

### 3.5. Court interventions

Another instrument the EDPS uses for giving effect to his role as an advisor to the EU institutions is the intervention in actions brought before the Court of Justice of the European Communities, under Article 47(1)(i) of Regulation (EC) No 45/2001. This instrument includes interventions before the Court of First Instance and the Civil Service Tribunal (although this last competence has not yet been used by the EDPS). The scope of this instrument was defined by the Court of Justice in its orders of 17 March 2005 in the PNR cases.

On 12 September 2007, an order of the president of the Court of Justice in case C-73/07 (*Satakunnan Markkinapörssi and Satamedia*) clarified that the competence of the EDPS does not extend to preliminary ruling proceedings. The EDPS has asked for leave to

intervene in this case concerning the meaning of 'processing of personal data carried out solely for journalistic purposes' laid down in Directive 95/46/EC.

On 8 November 2007, the Court of First Instance gave its judgment in case T-194/04 (*Bavarian Lager v Commission*), one of the three cases regarding the relationship between public access to documents and data protection in which the EDPS had intervened in 2006. The judgment represents an important milestone in the debates on this balance.

The Court of First Instance annulled the Commission's decision to refuse full access to the minutes of a meeting organised by the Commission, including the names of the participants of that meeting. The Court of First Instance held that disclosure of names of representatives of a collective body would not jeopardise the protection of their privacy and integrity.

The EDPS had intervened in the case in support of the applicant for access and had defended a position that was in substance confirmed by the Court of First Instance. In January 2008, the Commission issued an appeal at the Court of Justice.

Another case dealing with the legal basis of the data retention Directive 2006/24 (case C-301/06, *Ireland v Council and Parliament*), where the EDPS had requested to intervene in 2006, is still pending before the Court of Justice. In 2007, the EDPS issued written submissions.

Finally, in December 2007, the EDPS requested to intervene before the Court of First Instance in case T-374/07 (*Pachitis v Commission and EPSO*). The case is about the access of a person to the questions put to him and his answers when he took part in an open competition to constitute a reserve list for recruitment by the European institutions.

### 3.6. Other activities

#### The US–PNR agreement

The EDPS has been closely involved in the process leading to the agreement between the EU and the United States on the issue of PNR, as well as in various follow-up activities after the conclusion of the new agreement in July 2007.

<sup>(51)</sup> OJ L 199, 31.7.2007, p. 40.





Passenger data: not only used for flying, but also for finding criminals.

In the first place, the EDPS has commented on the negotiations mandate, whilst fully respecting the need for confidentiality. In the second place, he has actively participated in the activities of the Article 29 Working Party, inter alia in the preparation of a strategy paper on passengers data and in the organisation of a workshop in the European Parliament aimed at raising awareness on different aspects of the agreement. He also gave his view on the proposed agreement on several other occasions, for instance by giving (written and oral) evidence to the European Union Committee of the House of Lords.

Following the conclusion of the agreement, the EDPS has taken part, together with the other members of the Article 29 Working Party, in the analysis of the new agreement. In an opinion adopted by the working party on 17 August 2007, concerns were expressed on the fact that the safeguards in the new agreement had been weakened compared with the previous agreement.

In particular, the number and the quality of data transferred, the enlarged number of recipients, the lack of clarity with regard to the purpose for which data can be used and the conditions of review of the system were identified as raising specific concern. Since the opinion of the working party fully reflected the view of the EDPS, he abstained from presenting an EDPS opinion.

Benefiting from an active input of the EDPS, the working party has also been working on the conditions

for information to passengers when they buy a flight ticket. An opinion adopted on 15 February 2007<sup>(52)</sup> gives advice to airline companies on how to provide information by phone, in person and on the Internet. Model information notices have been drafted to facilitate this information, and to make sure the information provided is consistent across the EU.

### Implementing measures for SIS II

The legal instruments for a new Schengen information system (SIS II) confer powers on the Commission to establish implementing measures, including the preparation of the Sirene manual for the SIS II.

This manual covers some of the rules necessary for the proper functioning of the SIS II that cannot be exhaustively covered by the legal instruments because of their technical nature, the level of detail and the need for regular update. These rules complete the legal framework. Since these measures can have an impact on fundamental rights, the EDPS was informally consulted.

In his comments sent to the Commission on 7 September 2007, the EDPS addressed various issues such as:

- the communication of 'further information': clarification was needed on what was understood as 'further information' and on the need to provide for that kind of communication within the context of the Sirene manual;
- security measures: the EDPS took into consideration the high level of security requested by Article 10(1) of the legal instruments, and made several suggestions to increase the security requisites, especially as far as IT security is concerned;
- other topics, including: archiving, automatic deletion of data, change of purpose for an alert, requests for access to or rectification of the data, the interlinking of alerts, the procedures provided for in Article 25 of the Schengen Convention and statistics.

The informal comments were initially supposed to be followed by an opinion of the EDPS. However, the informal comments were discussed with the SIS-VIS Committee on 12 September 2007. They were taken into account to a reasonable extent. The comments that were not taken on board should be discussed again, with a view to assessing the possibility of includ-

<sup>(52)</sup> Opinion 2/2007 of the Working Party on Information to Passengers about Transfer of PNR data to US Authorities (WP 132).



ing them in a revised version of the implementing measures.

### Towards use of statistics

The EDPS adopted on 5 September 2007 an opinion on a proposal dealing with Community statistics on public health and health and safety at work (see paragraph 3.3.2). In his conclusions, the EDPS pointed out that a common review of the processes put in place in Eurostat when dealing with individual records for statistical purposes should be conducted and may lead to the need for prior checking.

In the EDPS' view, this common review should consist of the analysis of the minimum data set required for each processing operation and of an analysis of the processing operations implemented in Eurostat. Since then, several contacts have been made with the relevant departments of Eurostat in order to conduct this common review. Opinion 4/2007 of the Article 29 Working Party on the concept of personal data will be used as a background document in this context.

At the same time, the EDPS is being consulted on a proposal for a regulation of the European Parliament and of the Council on European statistics. This consultation is expected to run parallel with the common review, so that the EDPS will be able to draw general conclusions on the use of statistics.

### Consumer protection cooperation system and internal market information system

The EDPS has put a lot of effort in the data protection aspects of two large-scale IT systems for the exchange of information between Member States: the consumer protection cooperation system (CPCS) and the internal market information system (IMI).

The CPCS is an electronic database operated by the European Commission for the exchange of information among consumer protection authorities in Member States and the Commission pursuant to the provisions of Regulation (EC) No 2006/2004 on consumer protection cooperation<sup>(53)</sup>.

<sup>(53)</sup> Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the regulation on consumer protection cooperation), OJ L 364, 9.12.2004, p. 1.



Statistics can include personal information.

The IMI is another large-scale IT system operated by the European Commission to facilitate information exchanges between competent authorities in Member States in the area of internal market legislation. For the moment, information exchanges in IMI take place pursuant to Directive 2005/36/EC ('professional qualifications directive')<sup>(54)</sup> and Directive 2006/123/EC ('services directive')<sup>(55)</sup> only.

The EDPS first participated in the work of an ad hoc subgroup of the Article 29 Working Party, which resulted in two working party opinions on CPCS and IMI<sup>(56)</sup>. The EDPS served as a Rapporteur for the opinion on CPCS. Subsequently, in the autumn of 2007, the EDPS was closely involved in the preparation of:

- a Commission decision amending the implementing rules for the CPCS;
- a new Commission decision on the data protection aspects of IMI.

The EDPS supported the establishment of electronic systems for the exchange of information. Such streamlined systems may not only enhance efficiency of cooperation, but they may also help ensure compliance with applicable data protection laws. They may

<sup>(54)</sup> Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications, consolidated text published in OJ L 271, 16.10.2007, p. 18.

<sup>(55)</sup> Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ L 376, 27.12.2006, p. 36.

<sup>(56)</sup> WP 139 and WP 140 of 20 September 2007, published on the website of the working party.

do so by providing a clear framework on what information can be exchanged, with whom, and under what conditions.

Nevertheless, establishment of a centralised electronic system also creates certain risks. These include, most importantly, that more data might be shared and more broadly than strictly necessary for the purposes of efficient cooperation, and that data, including potentially outdated and inaccurate data, might remain in the electronic system longer than is necessary. The security of a database accessible in 27 Member States is also a sensitive issue, as the system is only as safe as the weakest link in the network permits it to be. Therefore, the EDPS recommended that data protection concerns should be addressed comprehensively both at the operational level and in legally binding Commission decisions for each system.

#### **RFID stakeholder group**

In May 2007, the EDPS was invited by the European Commission to join, as an observer, an RFID expert or stakeholder group launched for two years. The mission of the group is to assist the Commission in:

- preparing a recommendation, which has been its main activity in 2007;
- developing guidelines on how RFID applications should operate;
- assessing the need for further legislative steps;
- analysing the nature and the effects of the ongoing move towards the 'Internet of things';
- supporting the Commission's initiative to promote awareness campaigns.

The EDPS participated actively in the five meetings which were organised in 2007 and provided supportive analysis to the discussions of the group. The EDPS will continue to fuel the group in 2008, especially regarding the challenge of the 'Internet of things' and the governance issues of RFID.

#### **Data retention expert group**

The EDPS participated in the various meetings of the expert group on data retention. The 14th recital of the data retention Directive 2006/24 recognises that 'technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience

of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, *including the European Data Protection Supervisor*'.

The group will be formally established in 2008, but was already convened in 2007 and three sessions were held.

### **3.7. New developments**

The five perspectives for future change (interaction with technology, impact of the Lisbon Treaty, law enforcement, global privacy and jurisdiction, and full implementation of the directive), as defined in the EDPS opinion on the communication on the implementation of the data protection directive, will serve as the agenda for future activities of the EDPS.

#### **3.7.1. Interaction with technology**

In the 2005 annual report, the EDPS highlighted three technological trends the information society would increasingly rely upon for its development:

- (1) an everyday life environment made up of ubiquitous network access points;
- (2) an almost unlimited bandwidth; and
- (3) an endless storage capacity.

Since this statement, these emerging technological trends have started to produce some concrete developments which need to be closely followed as they are expected to have relevant impact on the EU data protection framework. Some of them are listed below.

#### **Trends**

In 1984, William Gibson<sup>(57)</sup> described a 'cyberspace' as a new and eventually parallel environment of the information society. More than 20 years later the information society can no longer be considered as a parallel world but rather as a growing, digitalised and integrated part of the daily life of almost every individual.

---

<sup>(57)</sup> *Neuromancer*, William Gibson, Ace edition, July 1984.



Data protection principles are equally applicable to digitised social space.

As stated in a recent article of *Firstmonday* <sup>(58)</sup>, a peer-reviewed journal on the Internet, the user/individual is seen as a main ‘producer’ of the new applications populating the so-called web 2.0 and these applications are fuelled by his/her personal data together with social and business interactions developed with others.

#### *The increase in ‘social computing’ applications*

The social life of individuals is increasingly digitalised through user-driven applications fed by data which are for the most part personal data. These applications, which give rise to web-based social networks, build their success on the number of users enrolled, the wealth of accurate data defining the stored profiles and of course their ability to enhance connections between individuals and content.

The EDPS considers this new application model as a technological development that is expected to have a major impact on data protection. It remains to be seen whether the existing European legal framework for data protection will provide sufficient protection. Specific attention has to be given to the concept of ‘controller’ (what meaning does this have when end users are the main actors processing data), the applicability of the regulation and the increasingly relative notion of location of the process. The EDPS welcomes the first position paper issued in 2007 by the European Network and Information Security Agency (ENISA) which presents some security issues and suggests rec-

<sup>(58)</sup> [http://www.firstmonday.org/ISSUES/issue12\\_3/pascul](http://www.firstmonday.org/ISSUES/issue12_3/pascul)

ommendations for social computing applications <sup>(59)</sup>.

Social computing or social networks also find their technical foundations in an earlier business environment driven by the development of remote applications and storage facility supported by huge data centres and server farms connected together in a so-called ‘cloud’ <sup>(60)</sup>.

#### *Data centres, virtualisation and remote data storage*

Supported by the three main technological trends identified previously which make their development possible, data centres may announce the end of the desktop where data, and more specifically personal data, have been processed until now. Remote data storage and web applications are already emerging, but the related data protection framework and the conditions for its proper application still need to be studied. Just as for social networks, the concept of the ‘location’ of the process and the identification of the ‘controller’ in the case of distributed computing resources become increasingly problematic.

When the processing of personal data, stored on peer-to-peer storage facilities, is spread over ‘cloud’ computing, the traditional implementation of the European data protection framework will find it increasingly difficult to enforce its underlying principles efficiently.

As underlined in his opinion on the implementation of the data protection directive <sup>(61)</sup>, the EDPS considers that in the light of these technological developments and in order to preserve innovations and foster new social interactions and business models, changes to the directive seem unavoidable, while keeping its core principles. Other administrative arrangements might be needed, which are on the one hand effective and appropriate to a networked society, and on the other hand minimise administrative costs.

<sup>(59)</sup> ‘Security issues and recommendations for online social networks’, October 2007, position paper No 1, ENISA ([http://www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_pp\\_social\\_networks.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf)).

<sup>(60)</sup> [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing)

<sup>(61)</sup> Discussed in Chapter 3.3 of the annual report.

## R & D

As privacy and data protection requirements need to be highlighted and applied as soon as possible in the life cycle of new technological developments, the EDPS considers that the European research and development (R & D) efforts constitute a very good opportunity to accomplish these goals and that the principle of ‘privacy by design’ should represent an inherent part of these R & D initiatives. The EDPS therefore conducted several actions in order to implement this principle in 2007.

### *Review of FP7 proposals*

In July 2007, at the request of the Commission, the EDPS reviewed some proposals in the seventh framework programme for research and technological development (FP7), answering the first call for tenders on ICT. Advice on data protection related aspects was provided on proposals which had already reached all thresholds.

### *Policy paper on R & D*

Early in 2008, the EDPS adopted a policy paper describing the possible role the institution could play for R & D projects in FP7. This document presents the selection criteria for the projects that qualify for an EDPS action and the ways in which the EDPS can contribute to these projects. Given the status of the EDPS as an independent authority, his participation as a partner of a consortium cannot be envisaged.

## 3.7.2. New developments in policy and legislation

### The impact of the Lisbon Treaty

The legal framework of the European Union is about to change with the entry into force of the Lisbon Treaty. This will also have consequences for the activities of the EDPS in his role as an advisor. The new treaty will determine a new context for these activities, which will have a particular impact on the proposals for legislation dealing with the exchange of personal data and the protection of these data for purposes of law enforcement.

The issues to be dealt with by the EDPS in 2008 include the following.

- How to act in the period of transition: important acts should not be adopted before the new treaty

(with qualified majority voting, co-decision and the availability of infringement procedures) is in place.

- What is the impact of the new treaty on areas where private parties are involved in law enforcement activities?
- Is a modification of Directive 95/46/EC and Regulation (EC) No 45/2001 needed?

### Law enforcement

The EDPS expects that the legislative activities relating to the increased need for storage and exchange of personal data for law enforcement purposes will continue. In his approach on these legislative activities, the EDPS will continue to analyse the justification of such legislative activities, on top of existing legislation that quite often has not even been fully implemented.

Alternative approaches might be needed, with other solutions to react to threats to society. Full implementation of existing legislation should always be an important consideration. The risks of new laws contributing to the emerging of a ‘surveillance society’ should be duly taken into account.

Another issue for the EDPS is the framework for data protection that — in spite of and perhaps also because of the adoption of the Council framework decision, probably in early 2008 — can be described as a patchwork. The framework is insufficient and it is unclear what rules apply to what specific situation. The same goes for the available remedies for the data subject.

### Global privacy and jurisdiction

In this context, it is useful to keep in mind the developments below.

- The exchange of information through open sources like the Internet is becoming more and more commonplace. It is not evident to what extent EU legislation is applicable and enforceable on the Internet, also since providers of services are quite often based outside the territory of the EU. As an example, search engines like Google or Yahoo can be mentioned.
- The transfer of personal data to third countries for law enforcement purposes, and even the access by authorities of third countries to data within the territory of the EU, is becoming increasingly important. The number of third countries requiring transfer or access is growing, for instance in relation to passenger data.

- There is no global consensus on common privacy standards. Recently, the first steps have been taken towards a common transatlantic approach.

As said in the EDPS opinion on the implementation of the data protection directive, the challenge will be to find practical solutions that reconcile the need for protection of the European data subjects with the territorial limitations of the European Union and its Member States.

A second challenge will be how to maintain the (high) level of protection within the EU also in relations with third countries: to what extent should we promote or give up our own standards, and to what extent should we negotiate common standards?

#### **Full implementation**

As explained in the EDPS opinion on the implementation of the data protection directive (see paragraph

3.3), full implementation includes a number of actions, which will also play an important role in the work of the EDPS in the coming years. A significant issue will in any event be the work on interpretative communications. These communications can contribute to a further harmonisation of the data protection laws in the Member States and also reveal topics for future changes of the directive.

Finally, the EDPS will actively participate in and, on some occasions, even initiate discussions on possible future changes of the data protection directive.

It is desirable to keep in mind that future changes might not only have implications for Directive 95/46/EC, but also for related instruments, such as Directive 2002/58/EC and Regulation (EC) No 45/2001.



## 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>(62)</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.

Further to its work programme for 2006–07 and with firm support of the EDPS, the working party concentrated on a number of strategic issues aiming at contributing to a common understanding of key provisions and ensuring a better implementation of them. The working party also improved the external communication about its own functioning. This resulted in various important documents, such as:

- working document on the processing of personal data relating to health in electronic health records (EHR), adopted on 15 February 2007 (WP 131);
- Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities, adopted on 15 February 2007 (WP 132);
- revised and updated policy to promote the transparency of the activities of the working party established by Article 29 of Directive 95/46/EC, adopted on 15 February 2007 (WP 135);
- Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP 136).

The working party issued a number of opinions on proposals for legislation or similar documents. In some cases, these subjects were also dealt with in opinions 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 opinions of the working party are also very useful, particularly since they may contain special points of attention from a national perspective.

The EDPS welcomes these opinions from the Article 29 Working Party, which have been consistent with his own opinions. In one case, the EDPS used his opinion to further develop certain elements of the

---

<sup>(62)</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.

working party's opinion. 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 3/2007 on the proposal for a regulation of the European Parliament and of the Council 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, adopted on 1 March 2007 (WP 134) <sup>(63)</sup>;
- Opinion 5/2007 on the follow-up agreement between the European Union and the United States on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, adopted on 17 August 2007 (WP 138);
- joint opinion on the proposal for a Council framework decision on the use of PNR for law enforcement purposes, presented by the Commission on 6 November 2007, adopted on 5 December 2007 (WP 145) <sup>(64)</sup>.

The EDPS and the working party have closely collaborated in the analysis of two new large systems in the first pillar, where supervisory tasks at EU and national level require a careful coordination:

- Opinion 6/2007 on data protection issues related to the consumer protection cooperation system (CPCS), adopted on 20 September 2007 (WP 139);
- Opinion 7/2007 on data protection issues related to the internal market information system (IMI), adopted on 20 September 2007 (WP 140).

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 assistance in the execution of their tasks. This cooperation takes place on a case-by-case basis. The SWIFT case continued to be a good example of multilateral cooperation, as the Article 29 Working Party was regularly monitoring the follow-up of its opin-

ion <sup>(65)</sup> adopted in 2006, and could eventually note substantial progress in ensuring compliance (see also paragraph 2.5).

The direct cooperation with national authorities is growing even more relevant in the context of large international systems such as Eurodac, which require a coordinated approach in supervision (see paragraph 4.3).

## 4.2. Council Working Party on Data Protection

In 2006, the Austrian and Finnish Presidencies convened a number of meetings of the Council Working Party on Data Protection. The EDPS welcomed this initiative as a useful opportunity to ensure a more horizontal approach in first pillar matters and contributed to several of these meetings.

The German Presidency decided to continue on the same basis with discussions on possible Commission initiatives and other relevant subjects in a first pillar context. In January 2007, it took the initiative for a questionnaire addressed to Member States on their experience with Directive 95/46/EC. About one half of the delegations replied to these questions. Their reactions confirmed that there is general satisfaction with the directive, although delegations also gave important feedback on potential problems and possible solutions. However, the German Presidency did not draw any specific conclusions.

In May 2007, the Commission presented its communications on the follow-up of the work programme for better implementation of the data protection directive, on promoting data protection by privacy enhancing technologies (PETs) and on radio frequency identification (RFID). Two of these communications have been the subject of EDPS opinions (see paragraph 3.3). The discussion in the Council working party did not give rise to different conclusions.

The EDPS used the first meeting under the German Presidency to present his priorities for consultation on new legislation (see paragraph 3.2). During the second meeting, the EDPS presented his 2006 annual report.

<sup>(63)</sup> See also EDPS opinion issued on 27 October 2006.

<sup>(64)</sup> The Working Party on Police and Justice (see paragraph 4.4) adopted this opinion on 18 December 2007. See also EDPS opinion issued on 20 December 2007.

<sup>(65)</sup> 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).

The Portuguese Presidency provided for one meeting of the working party, but it was cancelled. The Slovenian Presidency has also planned for one meeting in May 2008.

The EDPS continues to follow these activities with great interest and is available to advise and cooperate where appropriate.

### 4.3. Coordinated supervision of Eurodac

The cooperation with national data protection authorities, with a view to establishing a coordinated approach to the supervision of Eurodac, has developed rapidly since its start, only a few years ago.

The Eurodac Supervision Coordination Group (hereafter 'the group') is composed of representatives of the national data protection authorities and the EDPS, and met three times, namely in March, June and December 2007. It adopted some highly relevant documents for coordinated supervision, while the EDPS completed a security audit on Eurodac's Central Unit during the same period (see paragraph 2.10).

#### First coordinated inspection

At its first meeting in 2005, the group had decided to launch inspections at national level on specific elements of the Eurodac system. The results of this inspection would be compiled by the EDPS. The inspection was carried out in 2006 and was finalised in spring 2007. The report was published in July 2007<sup>(66)</sup>.

Three main issues — 'special searches', 'further use' and 'data quality' — were carefully scrutinised.

The group did not find indications for abuse of the Eurodac system. However, some aspects, such as information to the people concerned, need to be improved.

The report has been communicated to the main institutional stakeholders at EU level, and to international organisations and NGOs dealing with asylum and

- The use of 'special searches' is legally limited to those asylum-seekers and illegal immigrants who want to access their own personal data. The number of searches varied greatly between countries and there was concern about the high figures in some countries. The group concluded that there had been initial mistakes in the use of special searches, which have been corrected. The use of special searches should be monitored in the future, in order to avoid possible errors or abuse. The report also highlighted the need for raising awareness of the data subjects' rights.
- Eurodac fingerprints may only be used to determine the country responsible for an asylum application. No abuses were detected, despite the fact that some national Eurodac units are operated by police forces and despite the general increase of law enforcement authorities' access to databases. The group also found that in some countries there were difficulties in identifying the entity responsible for personal data processing, and the report recommends that steps are taken to resolve this.
- The quality of fingerprints is a basic requirement. The European Commission has expressed concerns about the fact that 6% of the fingerprints have been rejected due to low quality. The group concluded that the countries involved should take every step to ensure better quality, in terms of technology (live scans) as well as in terms of training.

immigration matters. The inspection had a noticeable impact on the number of special searches, which has dropped significantly in all Member States.

The EDPS considers this a positive experience, evidencing the good cooperation of the group and its ability to make a difference. This is not only important for the enforcement of asylum-seekers' rights to personal data protection, but also because this was a pilot exercise of great relevance for other large-scale

<sup>(66)</sup> See EDPS website: 'Supervision' section, under Eurodac.

information systems, such as the new Schengen information system (SIS II).

### Formalisation of working methods

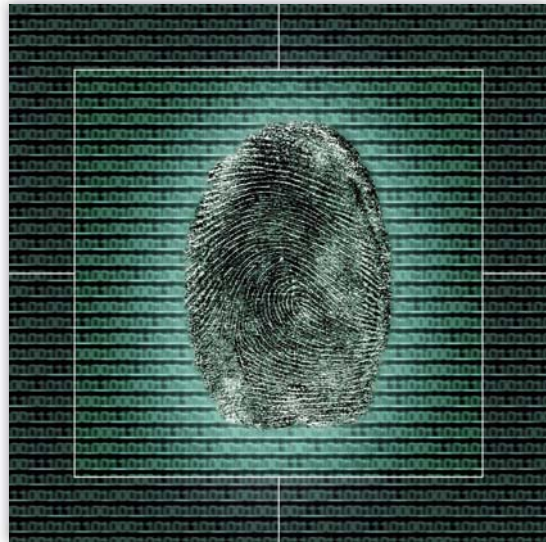
Initially, the group dealt with the coordinated supervision of Eurodac in an informal manner, based on the Eurodac regulation (Article 20) and the experience in other bodies. A more structured approach was felt necessary, for three main reasons.

- The model of coordinated supervision in the framework of Eurodac is likely to be used for other systems in the future. The legislative texts concerning these systems mention a coordinated supervision, where the authorities involved should define and develop their internal rules or working methods. Starting the reflection on these rules would allow more time for a step-by-step development.
- The review of the Dublin system by the Commission will lead to some legislative proposals concerning Eurodac. It is very likely that a part of the new legislation will concern the supervision of Eurodac. In this context, it would be logical for the European legislator to follow the same pattern as foreseen for other large-scale IT systems. Eurodac could thus benefit from a coordinated supervision on the same model, including the requisite of formalised working methods.
- Non-EU countries (e.g. Norway, Iceland and Switzerland) have joined or are about to join the system, including its supervision. These countries are not covered *expressis verbis* by the Eurodac regulation; their data protection authorities should be provided with a clear picture of the supervision model they enter into.

The EDPS tabled a list of key points for discussion at the March meeting. After discussion, a formal proposal for rules of procedure was analysed at the June meeting. It was agreed that the internal rules should at the same time provide clarity and flexibility. The rules of procedure should also avoid being unnecessarily heavy. They were adopted in December 2007.

### Future activities

There have been several significant new developments in 2007. The Commission issued the report on the Dublin evaluation in June, where the functioning of Eurodac was analysed and new perspectives suggested. On the other hand, there has been a growing pressure



Eurodac was established for the comparison of fingerprints of asylum applicants and illegal immigrants.

to give law enforcement authorities some access to Eurodac data. Both happened in the context of ongoing development of large-scale IT systems.

The group has identified its priorities among these developments: a work programme was adopted at the December meeting. The subjects for coordinated supervision are: information to data subjects, fingerprinting of children, and use of DubliNet. The advance deletion of data should also be examined later in 2008.

## 4.4. 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 (JSBs) 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 become apparent in recent years



through the increase of initiatives at European level to fight organised crime and terrorism, including different proposals for exchange of personal data.

In 2007, attention focused on two main subjects. The first one was the debate on the Commission proposal for a framework decision on data protection in the third pillar. The original proposal was discussed and revised, and the EDPS followed the developments very closely, issuing his third opinion on 27 April, and sending a letter to the Portuguese Presidency on 16 October (see paragraphs 3.3 and 3.4).

The Conference of European Data Protection Authorities, held in Larnaka (Cyprus) on 10–11 May 2007, adopted a declaration which was fully consistent with the EDPS opinion. European DPAs reaffirmed that creating a harmonised and high level of data protection covering police and judicial activities is crucial when establishing an area of freedom, security and justice. Furthermore, they regretted that the development of negotiations was leading to a narrow scope of application and an unsatisfactory level of data protection<sup>(67)</sup>.

The second subject was the exchange of law enforcement information in accordance with the principle of availability, and in particular the initiative of 15 Member States to make the Treaty of Prüm — laying down cross-border exchange of biometric data for combating terrorism and cross-border crime — applicable throughout the EU. The EDPS issued two opinions, on 4 April 2007 on the Prüm initiative itself, and on 19 December 2007 on its implementing rules (see paragraph 3.3).

In this context, the EDPS contributed to the common position of the European data protection authorities on the use of the concept of availability in law enforcement, adopted in Larnaka by the Conference of European Data Protection Authorities<sup>(68)</sup>. This declaration and an annexed checklist provide EU institutions and national parliaments with guidance about how to ensure that instruments on the principle of availability improve effectiveness in law enforcement, while ensur-

ing the fundamental right to the protection of personal data.

The conference in Larnaka also decided to confer a broader mandate to the Police Working Party, the working group following third pillar issues for the conference. The increasing need for constant monitoring, and for a fast and effective reaction to third pillar initiatives, call for a more stable and structured forum. The broader mandate of the Working Party on Police and Justice (the new name of the group) will include monitoring the developments in the area of law enforcement with regard to the processing of personal data, preparing all necessary actions to be taken by the conference in this area, as well as acting on behalf of the conference when a quick reaction is urgently needed. In this perspective, the conference appointed Mr Francesco Pizzetti, chairman of the Italian DPA, and Mr Bart De Schutter, member of the Belgian DPA, respectively as chairman and vice-chairman of the working party for a term of two years.

The EDPS actively contributed to the three meetings held by the Working Party on Police and Justice (WPPJ) during 2007. After agreeing on its rules of procedure and defining its working methods, the WPPJ dealt with various substantive issues:

- a letter to the Portuguese Presidency concerning the debate in Council about the framework decision on data protection in the third pillar;
- a first discussion on the implementing rules for the Prüm initiative;
- an opinion on the EU PNR proposal, adopted jointly with the Article 29 Working Party;
- the need for a common policy on supervision of law enforcement activities.

Furthermore, the EDPS and the chairman of the WPPJ both contributed to a meeting of the LIBE Committee of the European Parliament on the state of play on data protection in the third pillar.

## 4.5. European conference

Data protection authorities from EU Member States and the Council of Europe meet annually for a spring conference to discuss matters of common interest and to exchange information and experience on different topics. The EDPS and Assistant EDPS took part in the conference in Larnaka (Cyprus) on 10–11 May

---

<sup>(67)</sup> Declaration on the Draft Framework Decision on Data Protection in the Third Pillar, adopted on 11 May 2007, available on the EDPS website, 'Cooperation' section, under European Conference.

<sup>(68)</sup> Declaration on the Principle of Availability, with Common Position and Checklist, adopted on 11 May 2007, available on the EDPS website, 'Cooperation' section, under European Conference.



2007, hosted by the Commissioner for Personal Data Protection of Cyprus.

The EDPS contributed to the session focusing on 'Data protection in EU institutions'. Other subjects dealt with at the conference were: 'Electronic health records', 'Data protection, the way forward', 'Data protection in the third pillar', 'Media and personal data protection', 'Children and personal data', and other current issues. The conference adopted a number of important documents (see paragraph 4.4).

The next European conference will be held in Rome on 17–18 April 2008, and will take stock of relevant issues requiring attention.

Staff members participated in case handling workshops in Helsinki and Lisbon in April and November 2007. This interesting mechanism of cooperation at staff level — for exchange of best practices among European DPAs — is now in its ninth year. The next case handling workshop will be held in Ljubljana in March 2008.

#### 4.6. International conference

Data protection authorities and privacy commissioners from Europe and other parts of the world, including Canada, Latin America, Australia, New Zealand, Hong Kong, Japan and other jurisdictions in the Asia-Pacific region, have met annually for a conference in the autumn for many years. The 29th International Conference of Data Protection and Privacy Commissioners took place in Montreal on 25–28 September 2007 and was hosted by the Privacy Commissioner of Canada. It was attended by a large number of delegates from some 60 countries around the world.

The theme of the conference ('Privacy horizons: terra incognita') focused on the many challenging issues data protection and privacy commissioners are dealing with. The main challenges identified as 'dragons' were: 'Public safety', 'Globalisation', 'Law meets technology', 'Ubiquitous computing', 'Next generation' and 'Body as data'. Some workshop sessions explored possible answers, referred to as 'dragon slayers', such as 'Privacy impact assessments', 'Audits' and 'Children's privacy education'.

The EDPS and Assistant EDPS both attended the conference. The EDPS chaired a closed session for

Commissioners on the London initiative (see paragraph 4.7) and contributed to a workshop session on globalisation.

The conference adopted three resolutions<sup>(69)</sup>:

- on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes;
- on development of international standards (calling for closer involvement in ISO mechanisms); and
- on international cooperation (inter alia in cross-border enforcement and initiatives for raising awareness of data protection).

The next international conference will be in Strasbourg on 15–17 October 2008 and will be hosted jointly by the French data protection authority (CNIL) and the German Federal Commissioner for Data Protection and Freedom of Information.

#### 4.7. London initiative

At the 28th international conference in London in November 2006, a statement was presented, entitled 'Communicating data protection and making it more effective', which received general support from data protection authorities around the world. This was a joint initiative of the president of the French data protection authority (CNIL), the UK Information Commissioner and the EDPS (since then referred to as the 'London initiative'). As one of the architects of the initiative, the EDPS is committed to contribute actively to the follow-up with national data protection authorities<sup>(70)</sup>.

In the context of the London initiative, the president of the CNIL hosted a workshop on communication issues in Paris in February 2007. This resulted in the establishment of a network of communication officers for the exchange of experience and best practices in their field (see also paragraph 5.1).

The EDPS hosted a workshop on enforcement issues in Brussels in April 2007. The workshop dealt with three main issues:

- activities of DPAs in terms of inspections and audits;

<sup>(69)</sup> Available on the EDPS website, 'Cooperation' section, under International Conference.

<sup>(70)</sup> See 2006 annual report, paragraphs 4.5 and 5.1.

- further enforcement by way of interventions and sanctions; and
- possibilities for cross-border enforcement.

The latter part benefited from useful work undertaken by the Organisation for Economic Cooperation and Development (OECD). It became clear that data protection authorities are increasingly active in enforcement. The workshop highlighted valuable experience and best practices in this field.

At the international conference in Montreal (see paragraph 4.6), the EDPS chaired a closed session for commissioners devoted to the London initiative. Possibilities for further actions were discussed both for EU and Asia–Pacific regions. This underscored that the London initiative was meant to be truly global.

In December 2007, the UK Information Commissioner hosted a workshop in London focusing on effective strategies for data protection authorities. This workshop aimed at relevant issues for strategic planning and how to determine priorities for effective actions ('selective to be more effective').

The EDPS is pleased that these workshops are helping to make data protection more effective and to provide practical ways towards this strategic goal.

## 4.8. International organisations

International organisations are in many cases exempted from national laws. This often results in a lack of legal framework for data protection, even in those cases where very sensitive data are collected or exchanged between organisations. The international conference addressed this in a resolution in Sydney in 2003, calling for 'international and supranational bodies to formally commit themselves to (...) the principal international instruments dealing with data protection and privacy'.

The EDPS organised, together with the Council of Europe and the OECD, a workshop on data protection as part of good governance in international organisations in September 2005. The objective was to raise awareness of universal data protection principles and their consequences for international organisations. Representatives from some 20 organisations took part in discussions on the protection of personal data of staff and other persons concerned. Processing of sensitive data relating to health, refugee status or criminal convictions was also addressed.

The EDPS supported a second workshop organised by the European Patent Office in Munich in March 2007. Representatives from a variety of international organisations discussed issues of common relevance, such as the role of data protection officers, how to establish a data protection regime, and international cooperation with entities having different data protection standards.

The possibility of a third workshop in 2008–09 is presently under consideration.

## 5. Communication

### 5.1. Introduction

Information and communication activities continue to play a key part in the strategy and the daily work of the institution. Although not among the main roles of the EDPS, such as those covered in previous chapters, the crucial importance of information and communication activities for the practical impact of these roles can hardly be overstated. This is true at different levels. Basic **awareness of data protection** is a precondition for its continued wellbeing and effective application. Data subjects need to be aware of their specific rights, before they can make effective use of these rights. Responsible controllers need to be aware of their obligations, before they can ensure compliance. Institutional stakeholders need to be aware of the implications their policies may have on the protection of personal data and where data protection can contribute to more legitimacy and better results. Information and communication are finally also crucial tools for transparency about the EDPS' policies and activities.

The EDPS was one of the main architects of the '**London initiative**' designed to make communication on data protection, and data protection itself, more effective (see also paragraph 4.7). The EDPS followed this up in February 2007 by actively participating in the communication workshop hosted by the French data protection authority (CNIL). One significant result was the creation of a **network of communication officers** (with participation of the EDPS). Data protection authorities will be able to use this network to exchange best practices and to carry out specific projects, such as the development of joint actions for relevant events.

Another key aspect of data protection awareness is the **cooperation between the data protection officers** in

EU institutions and bodies. Close cooperation between DPOs is a resourceful method of sharing good practices and effectively working together to raise awareness on data protection issues among EU stakeholders and EU staff. The EPDS is keen to push this cooperation further by encouraging common actions and initiatives, for instance in the context of events like Data Protection Day. By working together in such a coherent manner, the impact of communication efforts can be enhanced to their full potential.

This chapter specifies the activities of the EDPS in 2007 in the area of information and communication, which encompassed the work of the press service, the use and development of online information tools (such as the website and the newsletter), attendance at workshops and conferences, the organisation of interviews, visits and press briefings, as well as media relations (for example, through the publication of relevant information materials and regular contact with journalists).

### 5.2. Communication 'features'

The EDPS' communication policy has to be shaped according to specific features that are relevant in view of the recent setting-up of the institution, its size and its remit. It thus follows a tailor-made approach, and uses the most appropriate tools to target the right audiences, whilst at the same time being adaptable to a number of constraints and requirements.

#### **Audience/target groups**

Unlike most other EU institutions and bodies, whose communication policies and activities need to operate on a general level, addressing EU citizens as a whole, the EDPS' direct sphere of action is much more

distinct. It is primarily focused at EU institutions and bodies, data subjects in general and EU staff in particular, EU political stakeholders, as well as 'data protection colleagues'. Therefore, the EDPS' communication policy does not need to engage in a 'mass communication' strategy. Instead, awareness around data protection issues among EU citizens in the Member States essentially depends upon a more indirect approach, mainly via data protection authorities at national level, and the use of information centres and contact points.

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

#### Language to be used

The EDPS' communication policy also needs to bear in mind the rather complex nature of its field of activity.

Data protection issues may indeed be viewed as fairly technical and obscure for non-experts, and the language in which we communicate should be adapted accordingly, especially when it comes to information and communication tools aimed at all sorts of audiences, such as the website and information leaflets. For such communication materials, as well as when drafting replies to information requests coming from citizens, a clear and comprehensible editing style which avoids unnecessary jargon needs to be used.

When considering more specialised audiences (the media, data protection specialists, EU stakeholders, etc.) technical and legal terms' usage is more relevant. In that sense, the 'same news' may require to be communicated using an adapted format and editing style, so as to rightly reflect the targeted audience (general public versus more specialised audience).

#### Impact

In order to make the most significant impact, the EDPS' communication style follows along the lines of 'too much information kills information', thereby prompting us to avoid 'over-communication'. The use

of 'traditional' communication tools (press releases, newsletters) is therefore voluntarily limited to issues that have greater significance, where it is deemed both necessary and timely to react and to inform the widest audience.

#### Visibility

As a recently established institution, increasing the EDPS' visibility on the EU political map was a clear focus of the EDPS' communication activities during his initial years of activity. In a relatively short period of time, a significant amount of work has been done to achieve this aim. Three years after the start of work, we can now see positive results in these communication endeavours.

One example of this is the selection of the EDPS as one of the *European Voice's* 50 nominees for the **2007 European of the Year** award, whose aim is to single out key European figures for the impact they have made on the EU agenda in that year. Peter Hustinx was recognised as having 'moved into a more proactive role, not hesitating to raise his voice, even in sensitive areas of security policy' <sup>(71)</sup>. His acknowledgement highlights the growth in awareness of the EDPS' actions and stance on sensitive data protection issues, which are high on the EU political agenda.

Moreover, the increased volume of requests for information and advice which the EDPS press service received on a daily basis in 2007 (see paragraph 5.5) further emphasises the view that the EDPS has become a point of reference for data protection issues.

### 5.3. Speeches

The EDPS continued to invest substantial 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.

The EDPS frequently appeared in the European Parliament's LIBE Committee or at related events. On 27 February, he presented his opinion on the proposal for a Council decision establishing the European Police

---

<sup>(71)</sup> See p. 45 of *Presenting the EV50 2007* magazine: [http://www.ev50.org/prs/EV50\\_Magazine\\_2007-pages28-54.pdf](http://www.ev50.org/prs/EV50_Magazine_2007-pages28-54.pdf)

Office (Europol). On 26 March, he spoke at a public seminar on PNR, SWIFT, Safe Harbor and transatlantic data protection. On 27 March, he contributed to a seminar on the common consular instructions and the use of biometrics. On 10 April, he intervened at a public hearing on the future of Europol. On 11 April, he presented his opinion on an initiative for a Council decision on cross-order cooperation, particularly in combating terrorism and cross-border crime, based on the Treaty of Prüm. On 7 May, he intervened at a public hearing on the Prüm decision. On 8 May, he presented his third opinion on the proposal for a Council framework decision on data protection in the third pillar. On 14 May, he presented his 2006 annual report. On 21 November, he commented on the general approach in the Council with regard to data protection in the third pillar. On 11 September, the Assistant EDPS presented the EDPS opinion on maintenance obligations at a joint hearing of LIBE and JURI and on 8 October he spoke at a LIBE public seminar on multi-level protection of fundamental rights.

On 16 January, the EDPS presented his priorities for consultation on new legislation to the Council Working Party on Data Protection. On 4 May, he was in Berlin for a discussion with the German Presidency on data protection in the first and third pillars. On 7 May, this discussion continued in Brussels with regard to data protection in the third pillar. On 24 May, the EDPS presented his 2006 annual report to the Council Working Party on Data Protection. On 4 September, he delivered a speech in Lisbon on 'Ethical issues relating to the use of biometrics' at a seminar organised by the Strategic Committee on Immigration, Frontiers and Asylum (SCIFA). On 13 March, the Assistant EDPS presented the EDPS opinion on Europol at the Council Working Party on Europol.

Other EU institutions and bodies were also on the list. On 22 March, the EDPS and the Assistant EDPS spoke at a meeting of the Secretary-General and the Directors-General of the European Commission on compliance with Regulation (EC) No 45/2001. On 26 April, he intervened at a plenary meeting of the Eurojust joint supervisory body. On 11 June, he spoke at a meeting of heads of agencies on compliance with Regulation (EC) No 45/2001. On 12 July, the EDPS and the Assistant EDPS visited Eurojust for a briefing on third pillar issues. On 7 December, the EDPS addressed the European Ombudsman's staff in Stras-



Peter Hustinx making a presentation to the European Financial Management and Marketing Association.

bourg. On 19 April, the Assistant EDPS made a presentation on medical data retention at a meeting of the College of Chiefs of Administration and on 24 April he presented the tasks and powers of the EDPS at a meeting of the assembly of staff committees of EU agencies, in Torrejón (Spain).

In the course of the year, the EDPS also visited a number of Member States. On 8 February, he delivered a speech at the Dutch Ministry of Justice in The Hague. On 2 April, he intervened at a colloquium on independent authorities in Athens. On 10 May, he spoke at the Spring Conference of European Data Protection Commissioners in Larnaka (Cyprus). On 15 May, he made a presentation at a seminar on advanced ID systems in Brussels. On 24 May, he delivered a speech on strategic issues in data protection at the European Data Protection Intensive in Amsterdam. On 7 June, he intervened at a conference on pharmaceutical compliance in Brussels. On 21 June, he made a presentation on the role of the EDPS to the Athens Bar Association. On 26 June, he spoke at a conference on RFID in Berlin.

On 2–3 July, the EDPS delivered speeches at the Privacy Law and Business Conference in Cambridge (UK). On 6 July, he was at the Institute of European Affairs in Dublin. On 13 July, he contributed to a twinning seminar on data protection in Sofia. On 24 August, he gave a speech at a privacy seminar in Cambridge (USA). On 6 September, he made a presentation at the UK Data Protection Forum in



London. On 14 September, he spoke at a Council of Europe seminar on judicial cooperation in Strasbourg. On 19 September, he delivered a speech at a conference on payment cards in Paris. On 20 September, he spoke at a EurActiv seminar in Brussels. On 27 September, he gave a speech at the International Conference of Data Protection and Privacy Commissioners in Montreal.

On 2 October, he presented a speech at a seminar of the European Biometrics Forum in Brussels. On 10 October, he spoke at a CEPS-Google panel discussion about online privacy in Brussels. On 11 October, he contributed to a conference on data protection compliance in London. On 13 October, he delivered a speech on the role of data protection authorities at the international conference 'Re-inventing data protection' in Brussels. On 22 October, he spoke at the conference 'Right to privacy in surveillance society' in Warsaw. On 26 October, he gave a speech on SIS II at a conference of Swiss data protection authorities in Solothurn. On 13 November, he contributed to a conference of the Lithuanian DPA in Vilnius. On 15 November, he spoke at a conference on RFID in Lisbon. On 10 December, he intervened at an ENISA seminar on data security in Brussels.

The Assistant EDPS made similar presentations. On 30 January, he made a presentation on new legislative proposals in the EU at a Data Protection Day seminar in Barcelona. On 16 February, he spoke at the CEPS seminar on mobility, control and new technologies in

Brussels. On 22 March, he gave evidence before a subcommittee of the House of Lords on PNR and the Treaty of Prüm. On 1 June, he took part in the workshop on privacy and the fight against terrorism organised by the Human Rights Commissioner of the Council of Europe (CoE), in Strasbourg. On 6 July, he spoke at the annual CEPS conference on democratic control and judicial accountability in the area of freedom, security and justice. From 12 to 14 September, he delivered several presentations in a CoE seminar on data protection and judicial cooperation and, on 14 September, he spoke at the European regional conference of Unesco-CoE on ethics and human rights in the information society. On 5 October, in Madrid, he made a presentation on the draft framework decision on data protection in the third pillar. On 10 October, he spoke at the ninth plenary meeting of the Lisbon network (training of judges) of the CoE. On 23 October, he delivered a speech on public access to documents and data protection, in Bilbao.

#### 5.4. Press service

Due to staff mobility, the press service experienced a certain degree of discontinuity in 2007, although internal arrangements were made so as to keep up with the ongoing work in the area of communications. A new press officer was recruited in December 2007 with a view to ensuring stability and professional development in press-related activities and communications.

The press service is in charge of external communication with the media through regular contacts with journalists. It also deals with requests for information and advice, writing press releases and newsletters, as well as organising press conferences and interviews with the EDPS or Assistant EDPS. In addition, the press officer leads a flexible information team which is involved in promotional activities and events (in particular the Data Protection Day and the EU Open Day; see paragraph 5.8), and in producing information materials aimed at the public and journalists.

In 2007, the press service issued 14 press releases — an average publication of one per month throughout the whole year. Most of them related to new legislative opinions which were of high public general relevance. Among the issues covered were the proposed frame-



Information team discussing the production of information materials.



Peter Hustinx and Joaquín Bayo Delgado presenting their Annual Report for 2006 during a press conference.

work decision on data protection in the third pillar, the inspection and audit of Eurodac, implementation of the data protection Directive 95/46/EC, the proposed road transport regulation, radio frequency identification (RFID), implementing rules of the Prüm Treaty, and the EU passenger name record (PNR) proposal.

Press releases are published on the EDPS website and distributed to a regularly updated network of journalists and interested parties. The information provided in the press releases usually results in significant media coverage, as they are often taken up in both the general and specialised press, in addition to being published on institutional and non-institutional websites ranging, among others, from EU institutions and bodies, to NGOs, academic institutions and IT companies.

A press conference was organised in early May 2007 to present the EDPS 2006 annual report to the press. The press conference highlighted that, after three years in operation, the EDPS had broadened his supervisory and consultative activities, and that the EU administration was now called upon to demonstrate that it

had made ‘substantial progress in complying with data protection obligations’.

## 5.5. Requests for information or advice

The number of requests for information or advice remained fairly stable during 2007, in comparison with 2006 (about 160 requests in 2007 compared with 170 in 2006). The requests for information or advice come from a wide range of individuals and actors, ranging from stakeholders operating in the EU environment and/or working in data protection (law firms, consultancies, associations, universities, etc.) to citizens asking for more information on privacy matters or requiring assistance for solutions to their questions or problems they are facing in the field.

A large majority of these requests were classified as ‘**requests for information**’ — a broad category which comprises, inter alia, general questions on EU policies and legislation, but also more specific issues relating to data protection in the Member States, as well as in the EU administration. By way of examples, requests

for information were received in 2007 concerning safety issues related to personal data, biometric technology, privacy on the Internet, transfer of personal data to third countries, access to EPSO personal details, as well as the implementation of Directive 95/46/EC in the Member States.

Requests that go beyond the informative aspect and which, therefore, require a more in-depth analysis are classified as ‘**requests for advice**’. In 2007, these accounted for a small minority (less than 5 % of the requests) and are usually dealt with by case officers. Advice was mainly sought by officials directly or indirectly dealing with data protection issues in the EU institutions and EU agencies. This obviously does not include the more substantial consultation on administrative measures (see paragraph 2.7).

Requests for advice received in 2007 covered the issue of public access to lists of admissible candidates in the European Parliament’s procedures, the nomination conditions of data protection officers, as well as data protection rules to be observed regarding the publication of pictures of participants to an event on a website.

As in previous years, most of the requests were received in English and, to a lesser extent, in French. This allowed for fast replies from the press service, well within the limit of 15 working days. However, a number of requests were also received in other EU official languages, which sometimes required the assistance of the Council’s translation service. In such cases, both the request and the reply went through translation so as to provide the author of the request with adequate information in his/her mother tongue.

## 5.6. Online information tools

### Website developments

The EDPS website remains its most important communication and information tool. It is also the medium through which visitors can access all the various documents produced within the framework of the EDPS’ activities (opinions, comments, work priorities, publications, speeches, press releases, newsletters, events’ information, etc.)

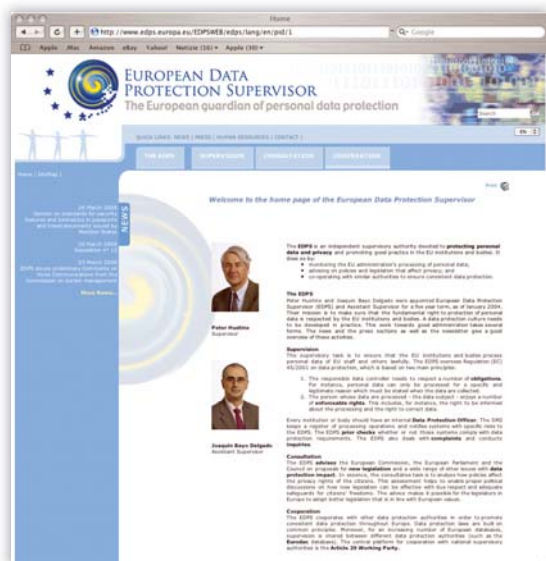
A new version of the EDPS website was launched in February 2007. It makes use of the web content man-

agement system (WCMS) technology, which is designed to facilitate the management of a large number of documents.

The welcome page, available in all Community languages, presents an introduction of the EDPS and his core tasks. The other pages of the website are presently available both in English and French. However, many documents available on the website are provided in all Community languages.

The website is divided into four sections.

- The first one (‘The EDPS’) contains general information about the EDPS and the Assistant EDPS as well as their mission, EU legislation specific to data protection and the EDPS publications, including the annual report, news and contact details.
- The other sections follow the division of the EDPS’ main tasks: the ‘Supervision’ section provides information and documents related to the monitoring of EU administrations’ processing of personal data. Among others, it contains a large number of the EDPS opinions that are issued following institutions’ notifications of processing operations presenting specific risks. The ‘Consultation’ section is related to the advisory role of the EDPS. Opinions on proposed legislation are published in the Official Journal and are available in all Community languages on the ‘Opinions’ subsection. The ‘Cooperation’ part reflects the work



Homepage of the new EDPS website.

undertaken in close collaboration with national data protection authorities, mostly at European or international level.

Further web functionalities, such as a register of notifications that was developed in 2007, will become public in 2008. Other information tools, such as a FAQ and a glossary, are also in the pipeline, with a view to further develop the content of the website and better meet visitors' expectations.

The EDPS press service continued to participate in the work of the Interinstitutional Internet Editorial Committee (CEiii) with a view to keep abreast of recent web technology developments.

### Newsletter

The EDPS newsletter provides news about the latest activities at the EDPS, such as opinions on EU legislative proposals and opinions on prior checks, together with relevant background and context. The newsletters are available on the EDPS website and an automatic subscription feature is also offered on the relevant page <sup>(72)</sup>.

Five issues of the EDPS newsletter were published in 2007, with an average frequency of about one issue every two months. The newsletter is published both in English and French.

The number of subscribers rose from around 460 people at the end of 2006 to a total of 635 at the end of 2007. Subscribers include, among others, Members of the European Parliament, EU staff and staff of national data protection authorities, as well as journalists, the academic community, telecommunication companies and law firms. This substantial and steady increase in the number of subscriptions since the newsletter was first published has induced the need to consider that time may be ripe to provide for an upgraded publication, that would include a more user-friendly design and layout. Such improvements will therefore be considered in the course of 2008.

The newsletter remains an efficient tool to draw attention to recent additions to the website as well as to raise awareness of the EDPS' latest activities. This in turn increases the visibility of the website and encourages subsequent visits. The newsletter is also a useful

device in the building-up of a community network interested in data protection activities at EU level.

## 5.7. Media contacts and study visits

The EDPS gave about 20 interviews to journalists of newspaper, broadcast or electronic media from different Member States or third countries, including the *Financial Times* and Associated Press, as well as Austrian, Danish, Dutch, German, Polish and UK radio or television. Moreover, news on EDPS activities frequently appeared in the *European Voice*, the *EU Reporter* and the internal publications of various institutions.

As part of the efforts aimed at further increasing his visibility, as well as interaction with the academic world, the EDPS welcomed visits from student groups specialised in the field of data protection and/or IT security issues. In May 2007, the EDPS for instance welcomed a group of German students to discuss issues of data protection in a 'surveillance society'. The EDPS and Assistant EDPS also contributed to the European Youth Media Days in June 2007.

## 5.8. Promotional events

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

### Data Protection Day

The EDPS, the EU institutions and national DPAs were invited in 2007 to notify the Council of Europe of the events they were planning to organise within the framework of the first European Data Protection Day.

The EDPS set up information stands at the European Parliament (on 25 January 2007) and the European Commission (on 26 January 2007) in order to raise awareness about data protection issues and the EDPS' activities among EU staff.

The EDPS took this opportunity to provide information about critical data protection issues at the time, such as passenger name record (PNR), SWIFT, the

<sup>(72)</sup> <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/27>





EDPS stand at the European Commission during Data Protection Day on 25 January 2007.



EDPS staff running the stand at the European Parliament during the EU Open Day on 5 May 2007.

Schengen information system (SIS), the visa information system (VIS), telecom data retention and camera surveillance. Special attention was given to the rights of the data subjects.

A poster was designed to feature the abovementioned data protection issues. Visitors to the EDPS stand were also invited to participate to a quiz about data protection in the EU institutions and bodies. A random draw determined the winners of a prize ('EDPS style' USB keys).

The first celebration of Data Protection Day on 28 January 2007 — unfortunately a Sunday that year — was initiated by the Council of Europe, with the support of the European Commission. The date marks the anniversary of the opening for signature of the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. The convention was the first legally binding international instrument in the field of data protection.

### EU Open Day

On 5 May 2007 in Brussels, the EDPS participated in the EU Open Day organised by the EU institutions and bodies to celebrate Europe Day (9 May).

The EDPS organised a stand at the European Parliament's premises and staff members were present to answer questions from visitors.

Various information materials presenting the EDPS' work were distributed to visitors, together with a range of promotional items (pens, stickers, mugs and USB keys displaying the EDPS logo). Visitors also had the opportunity to test their knowledge of data protection issues in a short quiz and to take part in a prize draw.



## 6. Administration, budget and staff

### 6.1. Introduction: developing the new institution

The development of the EDPS as a new institution <sup>(73)</sup> continued, with the aim of further consolidating its positive start. In 2007, the EDPS gained **additional resources** both in terms of budget (increasing from EUR 4 138 378 to EUR 4 955 726) and staff (from 24 in 2006 to 29 in 2007).

The **administrative environment** is gradually being extended on the basis of annual priorities, taking into account the needs and size of the institution. The EDPS has adopted new internal rules <sup>(74)</sup> necessary for the proper functioning of the institution. The Staff Committee is closely involved in the general implementing provisions of the Staff Regulations and other internal rules adopted by the institution. The Internal Auditor has communicated the conclusions of the first internal audit in 2007.

**Collaboration with other institutions** — the European Parliament, the Council and the European Commission — was further improved, allowing for considerable economies of scale. Slower performance of some tasks, connected to the principle of shared assistance (mainly related to access to administrative and financial software), was partly solved. The EDPS took over some of the tasks which were originally performed by other institutions.



Personnel, Budget and Administration Unit.

### 6.2. Budget

The budget adopted by the budgetary authority for 2007 amounted to EUR 4 955 726. This represents a 19.8 % increase compared with the budget for 2006.

In 2007, the EDPS prepared the renewal of its budget terminology, applicable for the establishment of the 2008 budget. It is based on the three years of experience of the EDPS, taking into account the specific needs of the institution and ensuring the transparency required by the budgetary authority.

The EDPS applies 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.

<sup>(73)</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) 45/2001.

<sup>(74)</sup> A list of administrative agreements and decisions is available in Annex I.

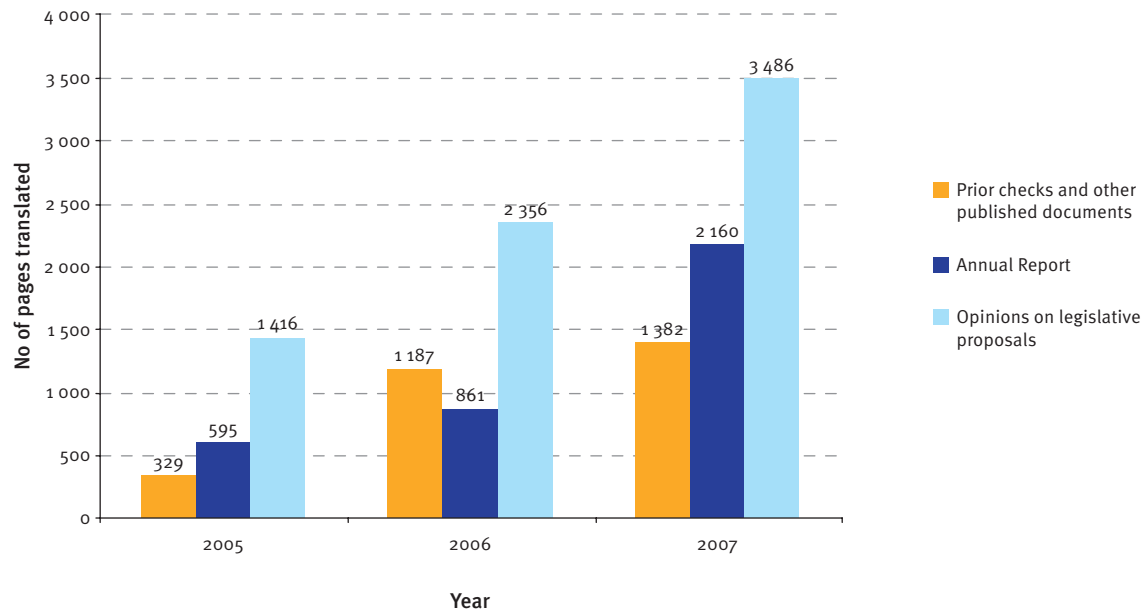


Table 1. Evolution of translation workload

Assistance from the Commission continued to be provided, particularly regarding the accounts, since the Accounting Officer of the Commission was also appointed as the Accounting Officer of the EDPS. As to financial software, the institution obtained direct access to a programme ('ABAC Workflow') allowing the processing of financial transactions from its premises.

In its report on the 2006 financial year, the European Court of Auditors stated that the audit had not given rise to any observations.

An important part of the budget is dedicated to translations, which have a substantial impact on the administrative work. EDPS opinions on legislative proposals are translated into 22 official European languages, with a temporary exception for Irish. These opinions are published in the *Official Journal of the European Union*. In 2007, the EDPS issued 12 opinions. Since 2005, the number of opinions has increased steadily, as well as the number of official languages. As a result, the number of pages to be translated has more than doubled.

Opinions on prior checks and other published documents are usually translated into the European institutions' working languages only. In 2007, the EDPS produced 151 official documents that required trans-

lation. This category of documents has more than tripled since 2005.

The number of missions carried out by the Members and EDPS staff has doubled since 2005. This is a logical consequence of the increase in activities of the institution. The administration team manages the financial aspects of the missions with help from the Paymaster's Office (PMO).

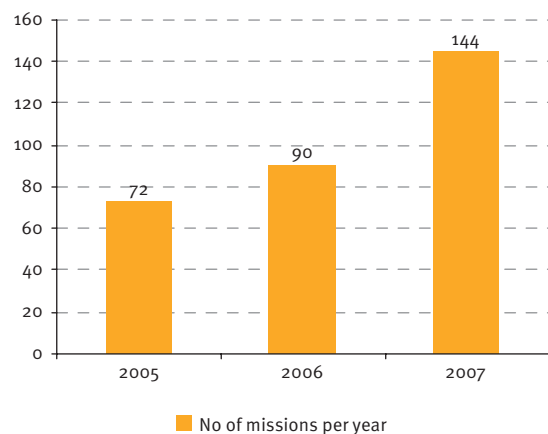


Table 2. Evolution of number of missions

### 6.3. Human resources

The EDPS benefits from the effective assistance of the Commission's services, regarding tasks relating to the personnel management of the institution (including two appointed members and 29 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 of the institution is leading to an increased workload, together with an expansion of tasks. The significant growth of the workload in 2007 has been described in previous chapters. Human resources obviously have a fundamental role to play in this context.

Nevertheless, the EDPS has chosen to restrict expanding in tasks and staff, using controlled growth to ensure that new staff are fully taken on board and adequately integrated and trained. For that reason, the EDPS called for the creation of only five posts in 2007 (four administrators and one assistant). This request was authorised by the budgetary authority, with the number of staff increasing from 24 in 2006 to 29 in 2007. Vacancy notices were published at the beginning of 2007 and all the posts were filled in the course of the year.

The Commission's assistance in this area has been valuable, particularly as regards the assistance of the PMO and Medical Service.

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

#### 6.3.2. Traineeship programme

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

The main programme hosts on average two trainees per session, with two five-month sessions per year (from

March to July and from October to February). The results of these sessions have been extremely positive.

In addition to the main traineeship programme, special provisions were established to accept university students and PhD students for a short-term period, as non-remunerated traineeships. This second part of the programme gives young students an opportunity to conduct research for their thesis. This is done in accordance with the 'Bologna process' and the obligation for these university students to complete a traineeship as part of their studies. At the end of 2007, a PhD student was selected for a two-month, non-remunerated traineeship. These traineeships are limited to exceptional situations and under stringent admission criteria.

All the trainees, whether remunerated or not, have contributed both in theoretical and practical work, while at the same time gaining first-hand experience.

On the basis of a service-level agreement signed in 2005, the EDPS has benefited from administrative assistance of the Commission's Education and Culture Directorate-General Traineeship Office, which has continued to provide valuable support thanks to the extensive experience of its staff.

#### 6.3.3. Programme for seconded national experts

The programme for seconded national experts (SNEs) was launched in January 2006, following the creation of its legal and organisational basis in autumn 2005 <sup>(75)</sup>.

The secondment of national experts enables the EDPS to benefit from the professional skills and experiences of staff from data protection authorities (DPAs) set up in the Member States. This programme enables national experts to familiarise themselves with data protection issues in the EU setting (in terms of supervision, consultation and cooperation). The benefit of this programme works both ways, as it also allows the EDPS to see his visibility increased at national level in the field of data protection.

In order to recruit national experts, the EDPS directly addresses the national DPAs. National permanent representations are also informed of the programme

<sup>(75)</sup> EDPS decision of 10 November 2005.

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.

In 2007, two national experts were seconded, one from the United Kingdom DPA — the Information Commissioner's Office — and another one from the Hungarian DPA — the Commissioner for Data Protection and Freedom of Information.

#### 6.3.4. Organisation chart

The EDPS' organisation chart has remained unchanged since 2004, namely: one unit, now consisting of eight people, which is responsible for administration, staff and the budget; and the remaining 21 members of staff who are in charge of the operational aspect of data protection tasks. They work under the direct authority of the EDPS and the Assistant EDPS in two main fields dealing with supervision and consultation.

Some flexibility has, however, been maintained in the allocation of tasks to staff, since the activities of the office are still developing.

#### 6.3.5. Training

A fundamental objective of staff training in the EDPS is to expand and improve individuals' competencies so that each staff member can optimally contribute to the achievement of the institution's goals. In 2007, the EDPS adopted an **internal training policy** based on the specific activities of the institutions, as well as on its strategic objectives. The general orientations, annexed to the corresponding decision, identify priority learning areas for the period 2007–08. The objective is to develop a 'centre of excellence' in the field of data protection and to improve staff knowledge and skills, so that EDPS values are fully integrated among the staff.

A welcome day for newcomers has been developed. It is based on a standard programme that provides a general view of the institution as well as the administrative environment to new colleagues.

EDPS staff have access to training courses organised by other European institutions and interinstitutional bodies, mainly the Commission and the European Administrative School (EAS).

The EDPS' participation at interinstitutional working parties (the EAS' Interinstitutional Working Party and the Interinstitutional Committee for Language Training) aims to share a common approach in a sector where the needs are essentially similar across the institutions and allow for economies of scale.

In 2007, the EDPS signed, together with the other institutions, a new protocol on the harmonisation of the cost of the interinstitutional language courses.

### 6.4. Administrative assistance and interinstitutional cooperation

Based on the interinstitutional cooperation agreement signed in June 2004 and extended in 2006 for a three-year period, interinstitutional cooperation remains crucial for the EDPS and his activities in terms of increased efficiency and economies of scale. This also allows avoidance of unnecessary multiplication of administrative infrastructures and reduction of unproductive administrative expenditures, whilst guaranteeing a high level of public service administration.

On this basis, interinstitutional cooperation continued in 2007 with various Commission DGs (Personnel and Administration DG; Budget DG; Internal Audit Service; Justice, Freedom and Security DG; Education and Culture DG), the Paymaster's Office, various European Parliament services (information and technology services, particularly with arrangements for the new version of the EDPS website; fitting out of the premises, building security, printing, mail, telephone, supplies, etc.) and the Council (regarding translation work).

Service-level agreements that were signed in 2005 with the various institutions and their departments are regularly updated. Agreements covering new areas are in preparation.

With a view to facilitating cooperation between Commission departments and the EDPS, and to improve the exchange of information between the services, direct access from EDPS premises to some of the Commission's financial management applications was requested in 2006 (ABAC, SAP). This direct access has been made possible for the ABAC system and is being developed for the SAP application. As regards human resources applications, there is still only partial

access to the Syslog system <sup>(76)</sup>. It is expected that full access will be made possible during 2008.

The remake of the EDPS website was developed in cooperation with the relevant services of the European Parliament. Nevertheless, problems related to the specific software that had been selected for its development have slowed down the finalisation of the project. The EDPS hopes to complete the project in the course of 2008.

Participation in the interinstitutional call for tenders for interim workers, insurance and furniture continued in 2007, allowing the institution to increase its efficiency in many administrative areas and to progress towards higher autonomy. Regarding office supplies, the EDPS participated in the European Parliament's call for tenders, which will lead to new contracts in summer 2008.

The EDPS continued to participate in various interinstitutional committees. However, because of the limited size of the institution, such participation had to be limited to only a few committees. This participation helped to increase the visibility of the EDPS in the other institutions and encouraged the continuous exchange of information and good practice.

## 6.5. Infrastructure

On the basis of the administrative cooperation agreement, the EDPS is located at the premises of the European Parliament, which assists the EDPS in the fields of information technology (IT) and telephone infrastructure.

The furniture and IT goods inventory has been set up with the help of the European Parliament services.

## 6.6. Administrative environment

### 6.6.1. Internal control system and audit

The process of identifying the risks related to the development of the EDPS' activities is clearly still at an early stage. The EDPS has adopted specific internal control

procedures deemed to be best suited to his needs on account of the size of the institution and its activities. The aim is to provide management and staff with a reasonable assurance for the achievement of its objectives and the management of the risks linked to its activities.

Overall, the EDPS considers that the internal control systems in place provide reasonable assurance on the legality and regularity of operations, for which the institution is responsible. The EDPS will ensure that its delegated authorising officer will continue her efforts to guarantee that reasonable assurance in the declarations accompanying the annual reports is effectively underpinned by appropriate internal control systems.

The first evaluation performed by the EDPS services has demonstrated the functionality and efficiency of the internal control system.

The first audit report made by the Internal Audit Service (IAS) was received in September 2007. It has confirmed the capacity of the EDPS internal control system to provide reasonable assurance for the achievement of the institution's objectives. Nevertheless, some aspects that needed to be improved were identified during the evaluation process. For some of these, prompt action has been undertaken, while others will progressively be put in place in the future along with the evolution of the tasks that are entrusted to the EDPS.

The implementation of IAS recommendations agreed by the EDPS is set as a priority for 2008. This will be undertaken on the basis of an action plan which will be drawn up early in 2008.

The EDPS intends to move further in this area with a view to keeping the level of risk for the institution down to a minimum.

### 6.6.2. Staff Committee

In accordance with Article 9 of the Staff Regulations of Officials of the European Communities, the EDPS adopted on 8 February 2006 a decision setting up a Staff Committee. The committee is consulted on a range of general implementing provisions for the Staff Regulations and on other internal rules adopted by the institution.

<sup>(76)</sup> Syslog is an information system for electronic management of training courses. ABAC and SAP are systems for accounting management.





EDPS Staff Committee during a meeting with the head of administration.

### 6.6.3. 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 relate to the fields for which the EDPS benefits from the assistance of the Commission, they are similar to those of the Commission, however with some adjustments to allow for the special nature of the EDPS' office. On the occasion of the welcome day, newly-recruited colleagues are provided with an Administrative Guide, which contains all the EDPS internal rules and informs them about the specificities of the institution. The document is regularly updated.

The EDPS continued to develop social facilities (mainly children related, such as crèches, access to the European School, etc.).

Two important internal decisions were adopted in 2007.

- Following an in-depth study of the evaluation systems of the other European institutions and a productive dialogue with the Staff Committee, the EDPS adopted Decision No 30 of 30 March 2007 setting out rules for the **evaluation** of his staff — according to the Staff Regulations of Officials of the European Communities <sup>(7)</sup>. A guide to staff

<sup>(7)</sup> Article 43: "The ability, efficiency and conduct in the service of each official shall be the subject of a periodical report (...)".

evaluation was prepared with a view to defining the evaluation criteria and the procedures for the reporting exercise. A mid-term interview has been introduced which allows for feedback after six months, giving the reported officer the possibility to improve his/her performance long before the official evaluation. Following the adoption of these rules, the first evaluation exercise was carried out in 2007.

- With the evaluation system in place, the implementation of a **promotion** system was the next logical step in the process aimed at creating and developing an administrative environment and a career structure. The EDPS adopted the rules governing the promotions system in Decision No 38 of 26 November 2007. Following the adoption of the decision, the first promotion exercise was carried out.

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

Additionally, a package of three decisions concerning staff **pension rights** was adopted. The EDPS opened the negotiations with the PMO for a delegation of day-to-day activities in this highly technical area.

### 6.6.4. Data protection officer

According to Article 24(1) of Regulation (EC) No 45/2001, the EDPS has appointed a data protection officer (DPO) to ensure the internal application of the provisions of the regulation. An inventory of operations involving processing of personal data was set up in 2007. The inventory aims to steer the notification process. On account of his specific position, the EDPS is developing a simplified notification process for cases subject to prior checking.

### 6.6.5. Document management

The EDPS started working on the implementation of a new electronic mail management system (GEDA), with the support of the European Parliament services.

This is intended as a first step in the development of a case-flow management system for improved support of EDPS activities.

## 6.7. External relations

As a European authority located in Brussels and recognised by the Belgian authorities, the EDPS, as well as his staff, benefit from the privileges and immunities laid down in the Protocol on the Privileges and Immunities of the European Communities.

## 6.8. Objectives for 2008

The objectives set for 2007 were fully achieved. In 2008, the EDPS will continue the consolidation process undertaken previously and further develop some activities.

The renewed **budget** terminology becomes effective in 2008. The EDPS plans the adoption of new internal financial rules adapted to its size. An optimisation of several internal handling processes is foreseen to keep the institution attuned to the steadily increasing quantity of financial files to treat. As to financial software, the EDPS will continue his efforts to acquire the tools allowing the access to financial files from his premises.

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 system and registration files will be developed and improved with the help of the Parliament services. Concerning human resources management software (mainly missions: MIPs; holidays and training: Syslog), the EDPS will equally make all the necessary efforts to acquire the programmes to allow access to the files from his premises.

The implementation of the improvements identified during the first assessment of the internal control system, as well as the implementation of the IAS recommendations received at the end of 2007, will be a priority. The DPO will continue to ensure the internal application of the provisions of Regulation (EC) No 45/2001.

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.

Additional **office space** will be needed in order to accommodate future staff. Negotiations to obtain enough space to cover the future needs will start with the European Parliament services in the course of 2008.

The EDPS intends to develop his social activities and finalise the development of the new website.



## 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 the Community institutions and bodies, and that an independent supervisory authority should be established.

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

## 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 countries of the Council of Europe, including all EU Member States.

Directive 95/46/EC was based on the principles of Convention 108, but specified and developed them in many ways. It aimed to provide a high level of protection and a free flow of personal data in the EU. When the Commission made the proposal for this directive in the early 1990s, it stated that Community institutions and bodies should be covered by similar legal safeguards, thus enabling them to take part in a free flow of personal data, subject to equivalent rules of protection. However, until the adoption of Article 286 of the EC Treaty, a legal basis for such an arrangement was lacking.

The appropriate rules referred to in Article 286 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 bod-

ies and on the free movement of such data, which entered into force in 2001 <sup>(78)</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 Treaty of Lisbon, signed in December 2007, enhances the protection of fundamental rights in different ways. Respect for private and family life and protection of personal data are treated as separate fundamental rights in Articles 7 and 8 of the EU Charter of Fundamental Rights that has been made legally binding. Data protection is also dealt with as a general provision in Article 16 of the Treaty on the Functioning of the EU. This clearly indicates that data protection is regarded as a basic ingredient of 'good governance'. Independent supervision is an essential element of this protection. See revised text in annex.

## 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.

The definitions and the substance of the regulation closely follow the approach of Directive 95/46/EC. It could be said that Regulation (EC) No 45/2001 is the implementation of that directive at European level. This means that the regulation deals with general principles like fair and lawful processing, proportionality and compatible use, special categories of sensitive data, information to be given to the data subject, rights of the data subject, obligations of controllers — addressing special circumstances at EU level where appropriate — and with supervision, enforcement and remedies. A separate chapter deals with the protection of personal data and privacy in the context of internal telecommunication networks. This chapter is in fact the implementation at European level of Directive 97/66/EC on privacy and communications.

<sup>(78)</sup> OJ L 8, 12.1.2001, p. 1.

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 the EDPS

The tasks and powers of the EDPS are clearly described in Articles 41, 46 and 47 of the regulation (see Annex B) both in general and in specific terms. Article 41 lays down the general mission of the EDPS — to ensure that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data are respected by Community institutions and bodies. Moreover, it sets out some broad lines for specific elements of this mission. These general responsibilities are developed and specified in Articles 46 and 47 with a detailed list of duties and powers.

This presentation of responsibilities, duties and powers follows in essence the same pattern as those for national supervisory bodies: hearing and investigating complaints, conducting other inquiries, informing controllers and data subjects, carrying out prior checks when

processing operations present specific risks, etc. The regulation gives the EDPS the power to obtain access to relevant information and relevant premises, where this is necessary for inquiries. He can also impose sanctions and refer a case to the Court of Justice. These **supervisory** activities are discussed at greater length in Chapter 2 of this report.

Some tasks are of a special nature. The task of advising the Commission and other 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 a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;
- (d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing

of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;

- (e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
- (f)
  - (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) also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;
- (g) participate in the activities of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of Directive 95/46/EC;
- (h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);
- (i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the data protection officers under Article 26;
- (j) carry out a prior check of processing notified to him or her;
- (k) establish his or her rules of procedure.

**Article 47 — Powers**

1. The European Data Protection Supervisor may:
  - (a) give advice to data subjects in the exercise of their rights;
  - (b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropri-

- ate, 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

|           |   |
|-----------|---|
| CCL       | common conservation list  |
| CdT       | Translation Centre for the Bodies of the European Union                           |
| CFCA      | Community Fisheries Control Agency  |
| CIS       | customs information system  |
| CoR       | Committee of the Regions  |
| CPCS      | consumer protection cooperation system  |
| CPVO      | Community Plant Variety Office  |
| DPA       | data protection authority   |
| DPC       | data protection coordinator (only in the European Commission)                     |
| DPO       | data protection officer   |
| EAS       | European Administrative School  |
| EC        | European Communities  |
| ECA       | European Court of Auditors  |
| ECB       | European Central Bank   |
| EESC      | European Economic and Social Committee  |
| EFSA      | European Food Safety Authority  |
| EIB       | European Investment Bank  |
| EMPL      | Committee on Employment and Social Affairs at the European Parliament             |
| ECHR      | European Convention on Human Rights   |
| ENISA     | European Network and Information Security Agency                                  |
| EMA       | European Medicines Agency   |
| EMCDDA    | European Monitoring Centre for Drugs and Drug Addiction                           |
| EMSA      | European Maritime Safety Agency   |
| EPSO      | European Personnel Selection Office   |
| ETF       | European Training Foundation  |
| EU        | European Union  |
| Eurofound | European Foundation for the Improvement of Living and Working Conditions          |
| EWS       | early warning system  |
| FIDE      | customs files identification database   |
| FP7       | seventh research framework programme  |
| IAS       | Internal Audit Service  |
| IGC       | Intergovernmental Conference  |
| IMI       | internal market information system  |
| JRC       | Joint Research Centre   |
| LIBE      | Committee on Civil Liberties, Justice and Home Affairs at the European Parliament |
| MoU       | memorandum of understanding   |
| OECD      | Organisation for Economic Cooperation and Development                             |
| OHC       | Occupation Health Centre  |
| OHIM      | Office for Harmonization in 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                                     |
| WP 29        | Article 29 Working Party                                    |
| WPPJ         | Working Party on Police and Justice                         |

## Annex D

## List of data protection officers (DPOs)

| 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   | Marc SCHAUSS           | dataprotectionofficer@curia.europa.eu  |
| European Court of Auditors   | Jan KILB               | data-protection@eca.europa.eu          |
| European Economic and Social Committee   | Sofia FAKIRI           | data.protection@eesc.europa.eu         |
| Committee of the Regions   | Petra CANDELLIER       | data.protection@cor.europa.eu          |
| European Investment Bank   | Jean-Philippe MINNAERT | dataprotectionofficer@eib.org          |
| European Investment Fund   | Jobst NEUSS            | j.neuss@eif.org                        |
| European Central Bank  | Martin BENISCH         | DPO@ecb.int                            |
| European Ombudsman   | Loïc JULIEN            | dpo-euro-ombudsman@ombudsman.europa.eu |
| European Data Protection Supervisor  | Giuseppina LAURITANO   | giuseppina.lauritano@edps.europa.eu    |
| European Anti-Fraud Office (OLAF)  | Laraine LAUDATI        | laraine.laudati@ec.europa.eu           |
| Community Fisheries Control Agency (CFCA)  | Rieke ARNDT            | rieke.arndt@ext.ec.europa.eu           |
| Community Plant Variety Office (CPVO)  | Véronique DOREAU       | doreau@cpvo.europa.eu                  |
| Education, Audiovisual and Culture Executive Agency  | Hubert MONET           | hubert.monet@ec.europa.eu              |
| European Agency for Reconstruction (EAR)   | Martin DISCHENDORFER   | martin.dischendorfer@ear.europa.eu     |
| European Agency for Safety and Health at Work (EU-OSHA)  | Terry TAYLOR           | taylor@osha.europa.eu                  |
| European Agency for the Management of Operational Cooperation at the External Border (Frontex) | Sakari VUORENSOLA      | sakari.vuorensola@frontex.europa.eu    |
| European Aviation Safety Agency (EASA)   | Arthur BECKAND         | arthur.beckand@easa.europa.eu          |
| European Centre for Disease Prevention and Control (ECDC)                                      | Elisabeth ROBINO       | elisabeth.robino@ecdc.europa.eu        |
| European Centre for the Development of Vocational Training (Cedefop)                           | Spyros ANTONIOU        | spyros.antoniou@cedefop.europa.eu      |
| European Environment Agency (EEA)  | Gordon McINNES         | gordon.mcinnnes@eea.europa.eu          |
| European Food Safety Authority (EFSA)  | Claus REUNIS           | dataprotectionofficer@efsa.europa.eu   |
| European Foundation for the Improvement of Living and Working Conditions (Eurofound)           | Markus GRIMMEISEN      | mgr@eurofound.europa.eu                |
| European GNSS Supervisory Authority (GSA)  | Dimitri NICOLAÏDES     | dimitri.nicolaides@gsa.europa.eu       |

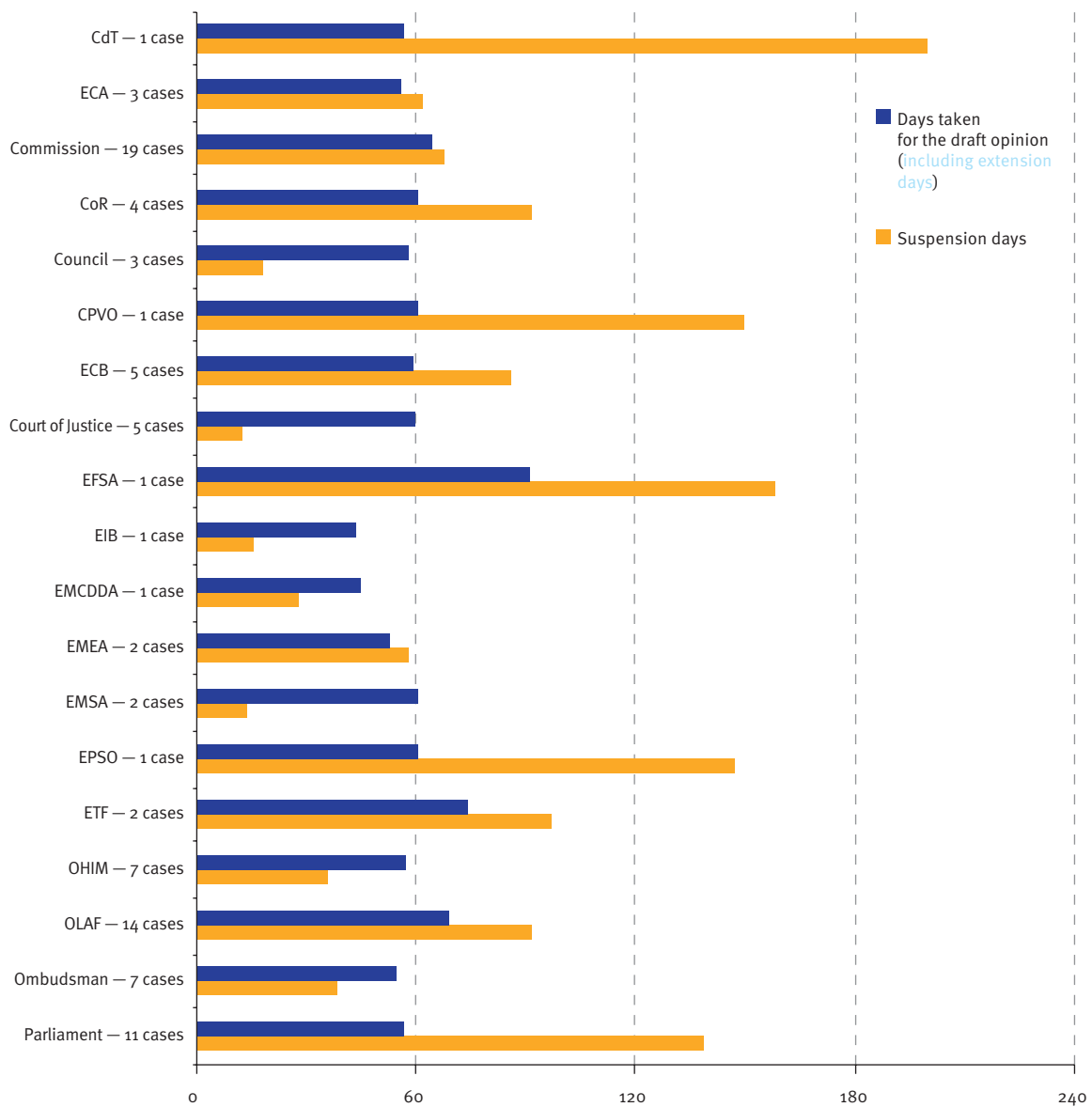
&gt;&gt;&gt;



| Organisation   | Name                   | E-mail                                |
|--|------------------------|---------------------------------------|
| European Maritime Safety Agency (EMSA)                           | Malgorzata NESTEROWICZ | malgorzata.nesterowicz@emsa.europa.eu |
| European Medicines Agency (EMA)                                  | Vincenzo SALVATORE     | data.protection@emea.europa.eu        |
| European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) | Cécile MARTEL          | cecile.martel@emcdda.europa.eu        |
| European Network and Information Security Agency (ENISA)         | Andreas MITRAKAS       | dataprotection@enisa.europa.eu        |
| European Railway Agency (ERA)                                    | Zografia PYLORIDOU     | zografia.pyloridou@era.europa.eu      |
| European Training Foundation (ETF)                               | <i>To be nominated</i> |                                       |
| European Union Agency for Fundamental Rights (FRA)               | Nikolaos FIKATAS       | nikolaos.fikatas@fra.europa.eu        |
| Executive Agency for Competitiveness and Innovation              | Olivier CORNU          | olivier.cornu@ext.ec.europa.eu        |
| Executive Agency for the Public Health Programme                 | Eva LÄTTI              | eva.latti@ec.europa.eu                |
| Office for Harmonization in the Internal Market (OHIM)           | Luc DEJAIFFE           | dataprotectionofficer@oami.europa.eu  |
| Translation Centre for the Bodies of the European Union (CdT)    | Benoît VITALE          | data-protection@cdt.europa.eu         |

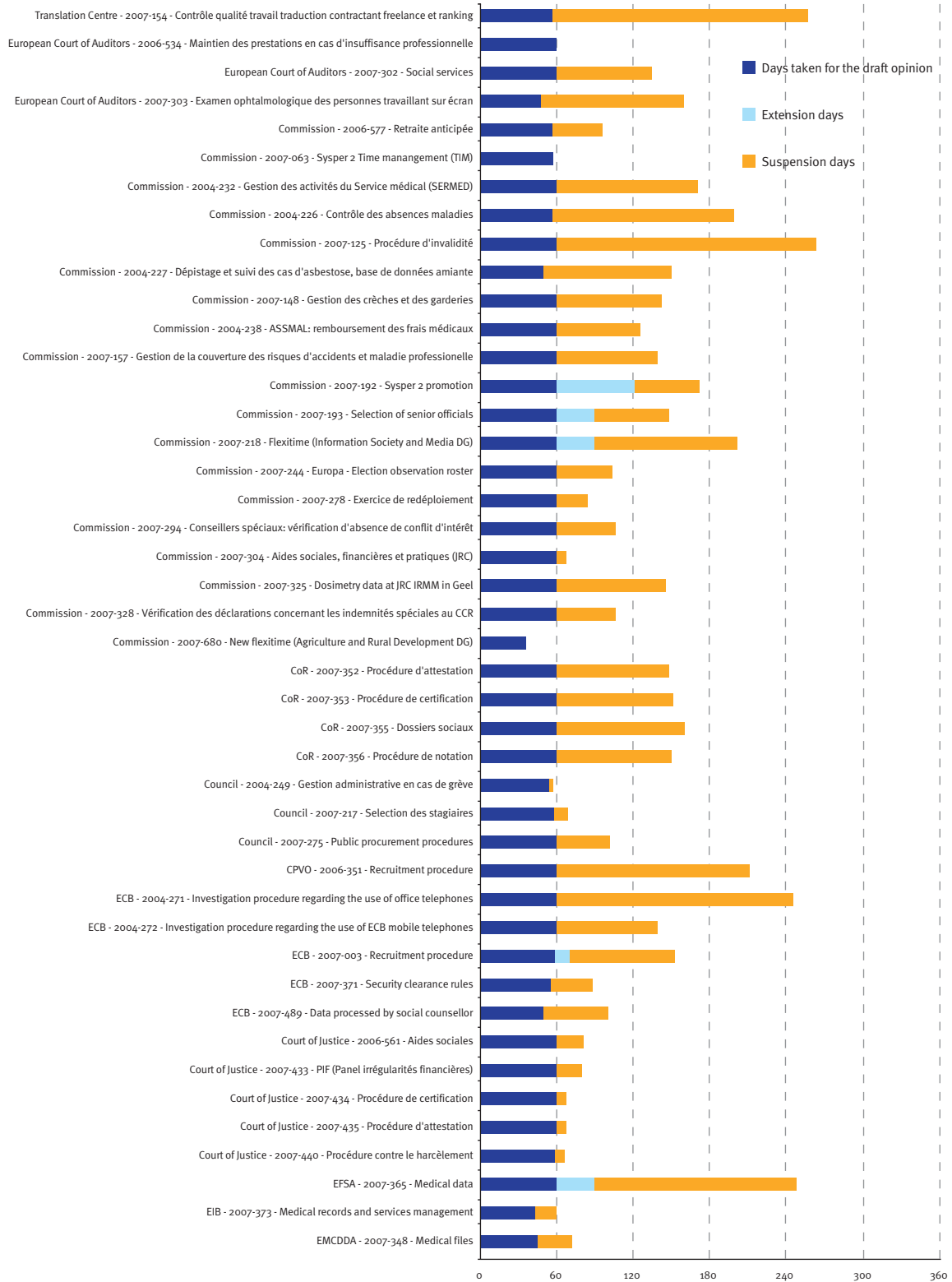
## Annex E

## Prior checking handling time per case and per institution

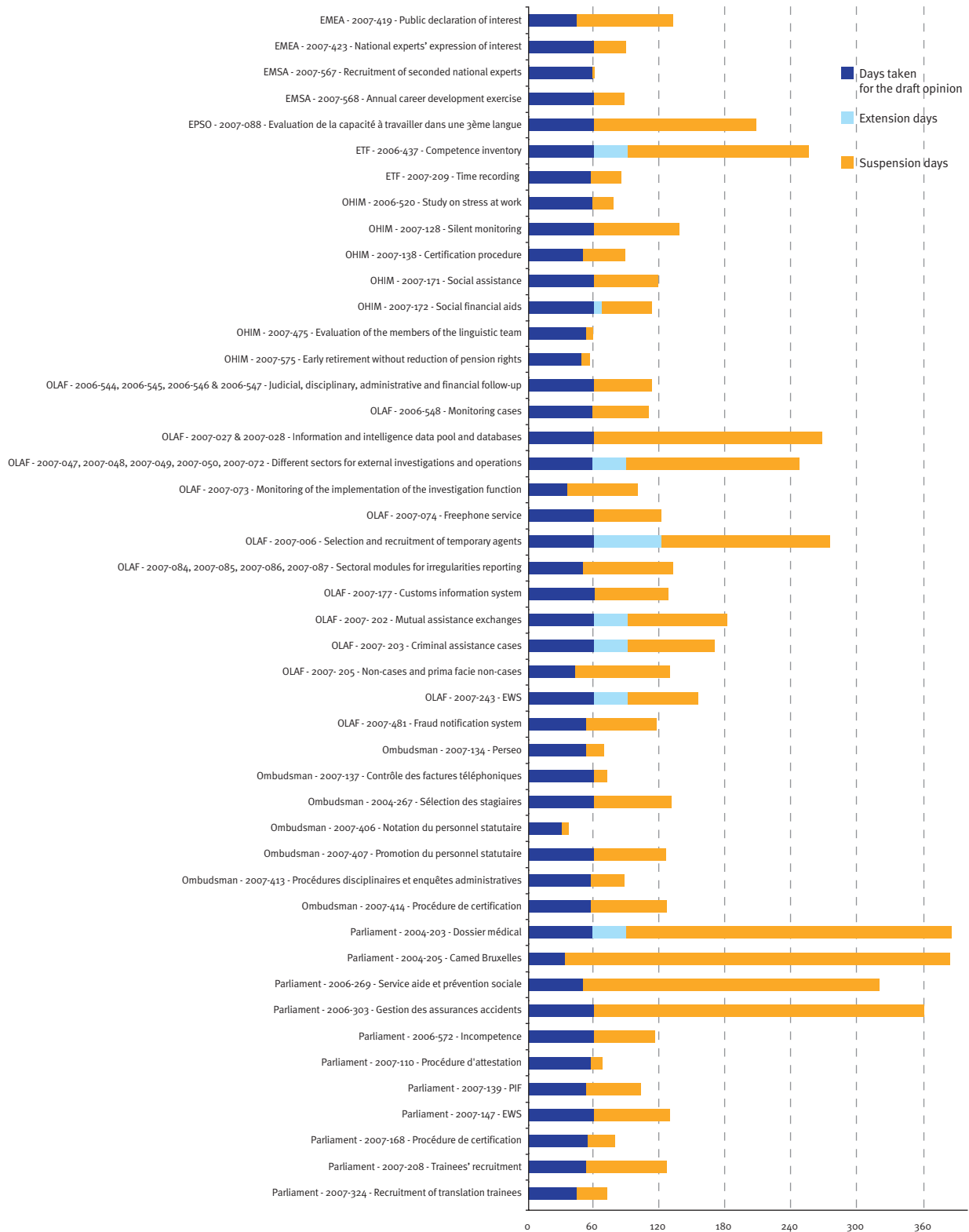


NB: Days taken for the draft opinions do not include the month of August in *ex-post* cases received before 1 September 2007. Suspension days include the suspension for comments on the draft, normally 7 to 10 days.

Opinions issued in 2007 (I)



**Opinions issued in 2007 (II)**



NB: Days taken for the draft opinions do not include the month of August in ex-post cases received before 1 September 2007. Suspension days include the suspension for comments on the draft, normally 7 to 10 days.

## Annex F

# List of prior check opinions

### **New flexitime AGRI — Commission**

Réponse du 19 décembre 2007 à une notification de contrôle préalable relative au 'New flexitime AGRI' (Dossier 2007-680)

### **Fraud notification service — OLAF**

Opinion of 18 December 2007 on a notification for prior checking on the fraud notification service (case 2007-481)

### **Career development — European Maritime Safety Agency**

Opinion of 17 December 2007 on a notification for prior checking concerning 'Annual career development' (case 2007-568)

### **Social counsellor — European Central Bank**

Opinion of 6 December 2007 on a notification for prior checking regarding the data processed by the social counsellor (case 2007-489)

### **Dossiers sociaux — CESE et CdR**

Avis du 6 décembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Dossiers sociaux' (Dossier 2007-355)

### **Procédure de notation — Comité des Régions**

Avis du 4 décembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Procédure de notation des fonctionnaires et agents' (Dossier 2007-356)

### **Procédure d'attestation — Comité des Régions**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'procédure d'attestation' (Dossier 2007-352)

### **Procédure d'invalidité — Commission**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Procédure d'invalidité — services médicaux Bruxelles — Luxembourg' (Dossier 2007-125)

### **Grève et actions assimilables — Conseil**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Gestion administrative en cas de grève et actions assimilables: retenues sur traitement et mesures de réquisitions' (Dossier 2004-249)

### **Dosimetry data at JRC-IRMM — Commission**

Opinion of 29 November 2007 on a notification for prior checking on 'Dosimetry data at JRC-IRMM in Geel' (case 2007-325)

### **Certification — Comité des Régions**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'procédure de certification' (Dossier 2007-353)



**Examen ophtalmologique — Cour des Comptes**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Examen ophtalmologique de suivi des personnes travaillant sur écran' (Dossier 2007-303)

**Early retirement — OHIM**

Opinion of 22 November 2007 on a notification for prior checking on the procedure for early retirement without reduction of pension rights (case 2007-575)

**Intelligence databases — OLAF**

Opinion of 21 November 2007 on a notification for prior checking on information and intelligence data pool and intelligence databases (joint cases 2007-27 and 2007-28)

**Recruitment of seconded national experts — EMSA**

Opinion of 20 November 2007 on a notification for prior checking regarding the recruitment procedure of seconded national experts (case 2007-567)

**Recruitment of temporary agents — OLAF**

Opinion of 14 November 2007 on a notification for prior checking regarding OLAF's selection and recruitment of its temporary agents (case 2007-6)

**Evaluation of the members of the linguistic team — OHIM**

Opinion of 12 November 2007 on a notification for prior checking on the evaluation of the members of the linguistic team (case 2007-475)

**Processing of personal data by social services — European Court of Auditors**

Opinion of 8 November 2007 on a notification for prior checking on processing of personal data by the social services (case 2007-302)

**National experts — EMEA**

Opinion of 26 October 2007 on a notification for prior checking regarding national expert's expression of interest (case 2007-423)

**Certification — Médiateur**

Avis du 24 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Procédure de certification' (Dossier 2007-414)

**Promotions — Médiateur**

Avis du 22 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Promotion du personnel statutaire' (Dossier 2007-407)

**Flexitime at Information Society and Media DG— Commission**

Opinion of 19 October 2007 on a notification for prior checking on the implementation of flexitime specific to the Information Society and Media DG (case 2007-218)

**Mutual assistance exchanges — OLAF**

Opinion of 19 October 2007 on a notification for prior checking on mutual assistance exchanges (case 2007-202)

**Procédure disciplinaire et enquête administrative — Médiateur**

Avis du 17 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'procédure disciplinaire et enquêtes administratives' (Dossier 2007-413)

**Irrégularités financières — Cour de justice**

Avis du 17 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'instance spécialisée en matière d'irrégularités financières' (Dossier 2007-433)

**Criminal assistance cases — OLAF**

Opinion of 12 October 2007 on a notification for prior checking on criminal assistance cases (case 2007-203)

**Absences pour maladie — Commission**

Avis du 11 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'contrôle des absences pour maladie Bruxelles-Luxembourg' (Dossier 2004-226)

**Sysper 2: promotions — Commission**

Avis du 9 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Sysper 2: promotions' (Dossier 2007-192)

**Early warning system — OLAF**

Opinion of 4 October 2007 on a notification for prior checking on the early warning system (case 2007-243)

**Indemnités spéciales au Centre Commun de Recherche — Commission**

Avis du 4 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Vérification des déclarations concernant les indemnités spéciales au Centre Commun de Recherche' (Dossier 2007-328)

**Harcèlement — Cour de justice**

Avis du 4 octobre 2007 sur la notification de contrôle préalable à propos du dossier 'procédure de harcèlement' (Dossier 2007-440)

**External investigations — OLAF**

Opinion of 4 October 2007 on five notifications for prior checking on external investigations (cases 2007-47, 2007-48, 2007-49, 2007-50, 2007-72)

**Procédure de certification — Cour de justice**

Avis du 3 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'procédure de certification' (Dossier 2007-434)

**Non-cases — OLAF**

Opinion of 3 October 2007 on a notification for prior checking on non-cases and prima facie non-cases (case 2007-205)

**Procédure d'attestation — Cour de justice**

Avis du 3 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier 'procédure d'attestation' (Dossier 2007-435)

**Selection of senior officials — Commission**

Opinion of 17 September 2007 on a notification for prior checking regarding the selection of senior officials (case 2007-193)

**Medical check-ups — EMCDDA**

Opinion of 13 September 2007 on the notification for prior checking regarding pre-employment and annual medical check-ups (case 2007-348)

**Conflict of interest of special advisers — Commission**

Opinion of 11 September 2007 on a notification for prior checking on verification of lack of conflict of interest of special advisers and its publication on the Europa website (case 2007-294)

**Service médical — Commission**

Avis du 10 septembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'gestion des activités du Service Médical-Bruxelles — Luxembourg- notamment via l'application informatique SERMED' (Dossier 2004-232)

**Security clearance — European Central Bank**

Opinion of 7 September 2007 on a notification for prior checking related to the application of the security clearance rules (case 2007-371)

**Exercices de redéploiement — Commission**

Avis du 5 septembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Interventions dans le cadre des exercices de redéploiement' (Dossier 2007-278)

**Evaluation de la troisième langue — EPSO**

Avis du 4 septembre 2007 sur la notification d'un contrôle préalable à propos du dossier 'Evaluation de la capacité à travailler dans une troisième langue (application de l'article 45.2 du Statut)' (Dossier 2007-88)

**Medical records and time management — European Investment Bank**

Opinion of 3 August 2007 on a notification for prior checking on the modification of the data-processing operations concerning 'gestion du temps' and 'medical records' (case 2007-373)

**Staff assessment — Ombudsman**

Opinion of 3 August 2007 on the notification for prior checking regarding staff assessment (case 2007-406)

**Recruitment of translation trainees — Parliament**

Opinion of 31 July 2007 on a notification for prior checking on the recruitment of translation trainees (case 2007-324)

**Trainee recruitment — Parliament**

Opinion of 31 July 2007 on a notification for prior checking on trainee recruitment (case 2007-208)

**Base de données 'Amiante' — Commission**

Avis du 27 juillet 2007 sur la notification d'un contrôle préalable à propos du dossier 'Dépistage et suivi des cas d'asbestose — Base des données 'Amiante' (Service Médical et interventions psychosociales BXL)' (Dossier 2004-227)

**Crèches — Commission**

Avis du 27 juillet 2007 sur la notification d'un contrôle préalable à propos du dossier 'Gestion des crèches et garderies à Bruxelles' (Dossier 2007-148)

**Accidents and occupational disease insurance — Commission**

Opinion of 27 July 2007 on a notification for prior checking related to administration of the accidents and occupational disease insurance (case 2007-157)

**Aides sociales (ISPRA) — Commission**

Avis du 24 juillet 2007 sur la notification d'un contrôle préalable à propos des aides sociales, financières et aide pratique (Dossier 2007-304)

**Customs information system — OLAF**

Opinion of 24 July 2007 on a notification for prior checking on the customs information system (case 2007-177)

**Social assistance — OHIM**

Opinion of 23 July 2007 on the notification for prior checking regarding the granting of social assistance (case 2007-171)

**Election observation roster — Commission**

Opinion of 23 July 2007 on a notification for prior checking on the Europa election observation roster (case 2007-244)

**Public procurement procedures — Council**

Opinion of 19 July 2007 on a notification for prior checking on the public procurement procedures (case 2007-275)

**Investigative function — OLAF**

Opinion of 19 July 2007 on a notification for prior checking on regular monitoring of the implementation of the investigative function (case 2007-73)

**Silent monitoring — OHIM**

Opinion of 18 July 2007 on a notification for prior checking on silent monitoring (case 2007-128)

**Système d'alerte précoce EWS — Parlement**

Avis du 16 juillet 2007 sur la notification d'un contrôle préalable à propos du dossier 'Système d'alerte précoce/early warning system (EWS)' (Dossier 2007-147)

**Monitoring cases — OLAF**

Opinion of 11 July 2007 on a notification for prior checking on monitoring cases (case 2006-548)

**Sickness insurance scheme**

Opinion of 10 July 2007 on a notification for prior checking related to management of the sickness insurance scheme (case 2004-238)

**Social financial aid — OHIM**

Opinion of 3 July 2007 on a notification for prior checking regarding the granting of 'social financial aid' (case 2007-172)

**AFIS system — OLAF**

Opinion of 29 June 2007 on a notification for prior checking on the use of dedicated sectoral modules on the AFIS system (cases 2007-84, 2007-85, 2007-86, 2007-87)

**Time recording system — ETF**

Opinion of 21 June 2007 on the notification for prior checking regarding ETF's time recording system (case 2007-209)

**Medical file (Brussels) — Parliament**

Opinion of 14 June 2007 on a notification for prior checking regarding the 'Camed-Brussels' (case 2004-205)

**Medical file (Luxembourg) — Parliament**

Opinion of 14 June 2007 on a notification for prior checking regarding the 'Medical file — Luxembourg' case (case 2004-203)

**Competence inventory — European Training Foundation**

Opinion of 13 June 2007 on a notification for prior checking regarding ETF's competence inventory (case 2006-437)

**Selection procedures for trainees — Council**

Opinion of 12 June 2007 on a notification for prior checking on the 'Selection procedure for trainees at the General Secretariat of the Council of the European Union' (case 2007-217)

**Financial irregularities panel — Parliament**

Opinion of 12 June 2007 on a notification for prior checking concerning the Financial Irregularities Panel (case 2007-139)

**Free phone service — OLAF**

Opinion of 6 June 2007 on a notification for prior checking on a free phone service (case 2007-74)

**Certification procedure — Parliament**

Opinion of 6 June 2007 on the notification for prior checking regarding the 'certification procedure' dossier (case 2007-168)

**Certification procedure — OHIM**

Opinion of 6 June 2007 on a notification for prior checking on the certification procedure (case 2007-138)

**Recruitment procedure — European Central Bank**

Opinion of 4 June 2007 on a notification for prior checking on recruitment procedure (case 2007-3)

**Verification of telephone bills — Ombudsman**

Opinion of 14 May 2007 on a notification for prior checking on verification of telephone bills (case 2007-137)

**Perseo — Ombudsman**

Opinion of 7 May 2007 on a notification for prior checking on Perseo (case 2007-134)

**Stress at work — OHIM**

Opinion of 2 May 2007 on a study on stress at work (case 2006-520)



**Welfare assistance — Parliament**

Opinion of 30 April 2007 on a notification for prior checking regarding 'Welfare assistance and guidance in the event of dependence' (case 2006-269)

**Accident insurance — Parliament**

Opinion of 30 April 2007 on a notification for prior checking concerning the 'Administration of accident insurance' (case 2006-303)

**Attestation procedure — Parliament**

Opinion of 26 April 2007 on a notification for prior checking on the attestation procedure (case 2007-110)

**Remedial procedure for incompetence — Parliament**

Opinion of 10 April 2007 on a notification for prior checking on remedial procedure for incompetence (case 2006-572)

**Time management — Commission**

Opinion of 29 March 2007 on the notification for prior checking on 'Sysper 2: Time management module' (case 2007-63)

**Follow-up data-processing operations — OLAF**

Opinion of 26 March 2007 on 'follow-up' data-processing operations (disciplinary, administrative, judicial, financial) (cases 2006-544, 2006-545, 2006-546, 2006-547)

**Medical check-ups — European Food Safety Authority**

Opinion of 23 March 2007 on the notification for prior checking regarding EFSA's pre-employment and annual medical check-ups (case 2006-365)

**Early retirement — Commission**

Opinion of 20 March 2007 on a notification for prior checking on the 'Annual exercise for early retirement without reduction of pension rights' dossier (case 2006-577)

**Use of mobile telephones — European Central Bank**

Opinion of 26 February 2007 on a notification for prior checking on investigation procedures regarding the use of mobile telephones (case 2004-272)

**Social aid — Court of Justice**

Opinion of 21 February 2007 on the notification for prior checking regarding social aid (case 2006-561)

**Use of office telephones — European Central Bank**

Opinion of 13 February 2007 on a notification for prior checking on investigation procedures regarding the use of office telephones (case 2004-271)

**Recruitment procedure — Community Plant Variety Office**

Opinion of 2 February 2007 on a notification for prior checking on recruitment procedure (case 2006-351)

**Incompetence — European Court of Auditors**

Opinion of 18 January 2007 on the notification for prior checking regarding the 'Maintaining professional standards in cases of incompetence' dossier (case 2006-534)

## Annex G

## List of opinions on legislative proposals

**European PNR**

Opinion of 20 December 2007 on the proposal for a Council framework decision on the use of passenger name record (PNR) data for law enforcement purposes

**Radio frequency identification (RFID)**

Opinion of 20 December 2007 on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on radio frequency identification (RFID) in Europe: steps towards a policy framework (COM(2007) 96)

**Implementing rules of Prüm initiative**

Opinion of 19 December 2007 on the initiative of the Federal Republic of Germany, with a view to adopting a Council decision on the implementation of Decision 2007/.../JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

**Road transport operator**

Opinion of 12 September 2007 on the proposal for a regulation establishing common rules concerning the conditions to be complied with to pursue the occupation of road transport operator, OJ C 14, 19.1.2008, p. 1

**Community statistics on health data**

Opinion of 5 September 2007 on the proposal for a regulation of the European Parliament and of the Council on Community statistics on public health and health and safety at work (COM(2007) 46 final), OJ C 295, 7.12.2007, p. 1

**Implementation of data protection directive**

Opinion of 25 July 2007 on the communication from the Commission to the European Parliament and the Council on the follow-up of the work programme for better implementation of the data protection directive, OJ C 255, 27.10.2007, p. 1

**Data protection in third pillar**

Third opinion of 27 April 2007 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, OJ C 139, 23.6.2007, p. 1

**Financing of the common agricultural policy**

Opinion of 10 April 2007 on the proposal for a Council regulation amending Regulation (EC) No 1290/2005 on the financing of the common agricultural policy (COM(2007) 122 final), OJ C 134, 16.6.2007, p. 1

**Cross-border cooperation (Prüm Treaty)**

Opinion of 4 April 2007 on the initiative of 15 Member States with a view to adopting a Council decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ C 169, 21.7.2007, p. 2

**Coordination of social security systems**

Opinion of 6 March 2007 on the proposal for a regulation laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems (COM(2006) 16 final), OJ C 91, 26.4.2007, p. 15

**Correct application of the law on customs and agricultural matters**

Opinion of 22 February 2007 on the proposal for a regulation amending Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (COM(2006) 866 final), OJ C 94, 28.4.2007, p. 3

**European Police Office**

Opinion of 16 February 2007 on the proposal for a Council decision establishing the European Police Office (Europol) (COM(2006) 817 final), OJ C 255, 27.10.2007, p. 13

## Annex H

## Composition of the EDPS Secretariat

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

Sophie LOUVEAUX  
*Administrator/Legal Officer*

Rosa BARCELÓ  
*Administrator/Legal Officer*

Zsuzsanna BELENYESSY  
*Administrator/Legal Officer*

Eva DIMOVNÉ KERESZTES  
*Administrator/Legal Officer*

Maria Veronica PEREZ ASINARI  
*Administrator/Legal Officer*

Jaroslav LOTARSKI  
*Administrator/Legal Officer*

Tereza STRUNCOVA  
*Administrator/Legal Officer*

György HALMOS (\*)  
*National Expert/Legal Officer  
(since September 2007)*

Delphine HAROU (\*)  
*Supervision Assistant*

Xanthi KAPSOSIDERI  
*Supervision Assistant*

Sylvie LONGRÉE  
*Supervision Assistant*

Kim Thien LÊ  
*Secretariat Assistant*

Thomas GREMEL  
*Supervision Assistant*

Stephen McCARTNEY  
*National Expert/Legal Officer  
(February 2007 to November 2007)*

Endre SZABÓ  
*National Expert/Legal Officer (until July 2007)*

• **Policy and Information**

Hielke HIJMANS  
*Administrator/Legal Officer*

Laurent BESLAY  
*Administrator/Technology Officer*

Bénédicte HAVELANGE  
*Administrator/Legal Officer*

Alfonso SCIROCCO  
*Administrator/Legal Officer*

Michaël VANFLETEREN  
*Administrator/Legal Officer*

Anne-Christine LACOSTE  
*Administrator/Legal Officer*

Nathalie VANDELLE (\*)  
*Administrator/Press Officer*

Per SJÖNELL (\*)  
*Administrator/Press Officer (until August 2007)*

Martine BLONDEAU (\*)  
*Documentation Assistant*

Andrea BEACH  
*Secretariat Assistant*

Matteo BONFANTI  
*Trainee (Oct. 2007 to Jan. 2008)*

Marie MCGINLEY  
*Trainee (March to July 2007)*

(\*) Information team



The European Data Protection Supervisor and the Assistant Supervisor with their staff.

**Personnel/Budget/Administration Unit**

Monique LEENS-FERRANDO  
*Head of Unit*

• **Human Resources/Administration**

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

Vittorio MASTROJENI  
*Human Resources Assistant*

Anne LEVÉCQUE  
*Human Resources Assistant*

Anne-Françoise REYNDERS  
*Human Resources Assistant*

• **Budget and Finance**

Tonny MATHIEU  
*Financial Administrator*

Raja ROY  
*Financial and Accounting Assistant*

Valérie LEAU  
*Accounting Assistant*



## Annex I

## List of administrative agreements and decisions

**Administrative agreement** signed by the Secretary-General of the European Parliament, of the Council and of the Commission and by the European Data Protection Supervisor (24 June 2004). Prolongation of this agreement signed on 11 December 2006.

### 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; 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 EDPS and the European Network and Information Security Agency (ENISA)
- Agreement on the harmonisation of the cost of the interinstitutional language courses
- Bilateral agreements between the European Parliament and the EDPS implementing the administrative agreement of 24 June 2004, prolonged 11 December 2006

### 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 the 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 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 the Supervisor adopting the rules laying down the procedure for implementing Article 45(2) of the Staff Regulations

Decision of 30 January 2007 of the Supervisor appointing the Data Protection Officer of the EDPS

Decision of 30 March 2007 of the Supervisor adopting general implementing provisions on staff appraisal

Decision of 18 July 2007 of the Supervisor adopting the internal training policy

Decision of 1 October 2007 of the Supervisor appointing the Accounting Officer of the EDPS

Decision of 1 October 2007 of the Supervisor for implementing Article 4 of Annex VIII of Staff Regulations on pension rights

Decision of 1 October 2007 of the Supervisor for implementing Articles 11 and 12 of Annex VIII of Staff Regulations on transfer of pension rights

Decision of 1 October 2007 of the Supervisor for implementing Article 22(4) of Annex XIII of Staff Regulations on pension rights

Decision of 12 September 2007 of the Supervisor on the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Communities' interests

Decision of 9 November 2007 of the Supervisor appointing the Internal Auditor of the EDPS

Decision of 26 November 2007 of the Supervisor adopting general implementing provisions on promotions

European Data Protection Supervisor

**Annual Report 2007**

Luxembourg: Office for Official Publications of the European Communities

2008 — 106 pp. — 21 × 29.7 cm

ISBN 978-92-95030-38-1

### **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.



EUROPEAN DATA  
PROTECTION SUPERVISOR

QT-AA-08-001-EN-C

*The European guardian  
of personal data protection*  
**[www.edps.europa.eu](http://www.edps.europa.eu)**

