

# Annual Report

## 2008



EUROPEAN DATA  
PROTECTION SUPERVISOR





# Annual Report

## 2008



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, 2009

ISBN 978-92-95073-02-9

doi: 10.2804/55407

© Photos: Sylvie Picart-Longrée et iStockphoto

© European Communities, 2008

Reproduction is authorised provided the source is acknowledged.

*Printed in Italy*

PRINTED ON WHITE CHLORINE-FREE PAPER

# Contents

User's guide	7
Mission statement	9
Foreword	11
1. Balance and perspectives	13
<b>1.1. General overview of 2008</b>	<b>13</b>
<b>1.2. Results in 2008</b>	<b>15</b>
<b>1.3. Objectives in 2009</b>	<b>16</b>
2. Supervision	17
<b>2.1. Introduction</b>	<b>17</b>
<b>2.2. Data protection officers</b>	<b>17</b>
<b>2.3. Prior checks</b>	<b>19</b>
2.3.1. Legal base	19
2.3.2. Procedure	19
2.3.3. Quantitative analysis	21
2.3.4. Main issues in <i>ex post</i> prior-check cases	25
2.3.5. Main issues in proper prior checks	31
2.3.6. Consultations on need for prior checking	34
2.3.7. Notifications not subject to prior checking or withdrawn	35
2.3.8. Follow-up of prior-check opinions	36
2.3.9. Conclusions and the future	37
<b>2.4. Complaints</b>	<b>37</b>
2.4.1. Introduction	37
2.4.2. Cases declared admissible	38
2.4.3. Cases not admissible: main reasons for inadmissibility	42
2.4.4. Collaboration with the European Ombudsman	43
2.4.5. Further work in the field of complaints	44
<b>2.5. Inspection policy</b>	<b>44</b>
2.5.1. Spring 2007 and beyond	44
2.5.2. Inspections	45
<b>2.6. Administrative measures</b>	<b>48</b>
2.6.1. New model of the medical certificate	48
2.6.2. Access to documents	48
2.6.3. Special categories of data: applicable law	49
2.6.4. Request from a court for a copy of the full medical file of an official	49
2.6.5. Retention of data-related disciplinary penalties	50
2.6.6. Implementing rules of Regulation (EC) No 45/2001	51
2.6.7. Complaints handled by the European Ombudsman	51
<b>2.7. Video-surveillance</b>	<b>51</b>
2.7.1. Guidelines	51
2.7.2. Prior checking	52
2.7.3. Complaint	52
2.7.4. Other requests	53
<b>2.8. Eurodac</b>	<b>53</b>

3. Consultation	54
<b>3.1. Introduction</b>	<b>54</b>
<b>3.2. Policy framework and priorities</b>	<b>55</b>
3.2.1. Implementation of consultation policy	55
3.2.2. Inventory 2008	56
3.2.3. Inventory 2009	57
<b>3.3. Legislative opinions</b>	<b>58</b>
3.3.1. General remarks	58
3.3.2. Individual opinions	59
<b>3.4. Comments</b>	<b>65</b>
<b>3.5. Court interventions</b>	<b>66</b>
<b>3.6. Other activities</b>	<b>67</b>
3.6.1. E-privacy	67
3.6.2. PNR	68
3.6.3. Implementation SIS and border policy	68
3.6.4. Conference on data protection and law enforcement (Trier)	68
3.6.5. EU RTD	69
3.6.6. Google / DoubleClick Merger and data protection issues	70
3.6.7. Participation in expert groups	71
3.6.8. Maritime accidents	71
3.6.9. Communicable diseases	72
3.6.10. The Community Customs Code and the Economic Operators and Registration number (the EORI number)	72
<b>3.7. New developments</b>	<b>72</b>
3.7.1. Interaction with technology	72
3.7.2. New developments in policy and legislation	75
4. Cooperation	77
<b>4.1. Article 29 Working Party</b>	<b>77</b>
<b>4.2. Council Working Party on Data Protection</b>	<b>78</b>
<b>4.3. Coordinated supervision of Eurodac</b>	<b>79</b>
<b>4.4. Third pillar</b>	<b>80</b>
<b>4.5. European conference</b>	<b>81</b>
<b>4.6. International conference</b>	<b>81</b>
<b>4.7. London initiative</b>	<b>82</b>
<b>4.8. International organisations</b>	<b>83</b>
5. Communication	84
<b>5.1. Introduction</b>	<b>84</b>
<b>5.2. Communication ‘features’</b>	<b>85</b>
<b>5.3. Speeches</b>	<b>86</b>
<b>5.4. Media relations</b>	<b>89</b>
<b>5.5. Requests for information</b>	<b>90</b>
<b>5.6. Study visits</b>	<b>91</b>
<b>5.7. Online information tools</b>	<b>91</b>
<b>5.8. Publications</b>	<b>92</b>
<b>5.9. Awareness-raising events</b>	<b>93</b>
<b>5.10. Priorities for 2009</b>	<b>94</b>

6. Administration, budget and staff	95
<b>6.1. Introduction</b>	<b>95</b>
<b>6.2. Budget</b>	<b>95</b>
<b>6.3. Human resources</b>	<b>96</b>
6.3.1. Recruitment	96
6.3.2. Traineeship programme	96
6.3.3. Programme for seconded national experts	97
6.3.4. Organisation chart	97
6.3.5. Social dialogue	97
6.3.6. Training	97
6.3.7. Social activities	98
6.3.8. Protocol on the privileges and immunities of the European Communities.	98
<b>6.4. Control functions</b>	<b>98</b>
6.4.1. Internal control	98
6.4.2. Internal audit	99
6.4.3. Security	99
6.4.4. Data Protection Officer	99
<b>6.5. Infrastructure</b>	<b>99</b>
<b>6.6. Administrative environment</b>	<b>99</b>
6.6.1. Administrative assistance and inter-institutional cooperation	99
6.6.2. Internal rules	100
6.6.3. Document management	101
<b>6.7. Objectives for 2009</b>	<b>101</b>
Annex A — Legal framework	103
Annex B — Extract from Regulation (EC) No 45/2001	105
Annex C — List of abbreviations	107
Annex D — List of data protection officers (DPOs)	109
Annex E — Prior checking handling time per case and per institution	111
Annex F — List of prior-check opinions	115
Annex G — List of opinions on legislative proposals	123
Annex H — Composition of the EDPS's Secretariat	125
Annex I — List of administrative agreements and decisions	127





# User's guide

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

**Chapter 1 — Balance and perspectives** presents a general overview of the activities of the EDPS. This chapter also highlights results achieved in 2008 and puts forward the main objectives for 2009.

**Chapter 2 — Supervision** extensively describes the work done to ensure and monitor the Community 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 presents an analysis of prior checks (both quantitative and on substance), complaints, inspection policy and advice on administrative measures dealt with in 2008. It also 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's advisory role, focusing on opinions and comments 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: it sets out some new technological issues and highlights new developments in policy and legislation.

**Chapter 4 — Cooperation** describes work done in key forums such as the Article 29 Data Protection Working Party, in the joint supervisory authorities of the 'third pillar', and at the European as well as the international data protection conferences.

**Chapter 5 — Communication** presents the EDPS's information and communication activities and achievements, including the work of the press service and external communication with the media. 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's organisation, including budget issues, human resources matters and administrative agreements.

The report is completed by a number of **annexes**, which provide an overview of the relevant legal framework, provisions of Regulation (EC) No 45/2001, a list of abbreviations and acronyms used in the report, statistics regarding prior checks, the list of DPOs of EU institutions and bodies, as well as the composition of the EDPS's 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's activities in 2008.

Those who wish to get further details about the EDPS are encouraged to visit our website which remains our most prominent tool of communication (<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 free of charge from EU Bookshop (<http://www.bookshop.europa.eu>) or from the EDPS. Contact details are available on our website, under the 'Contact' section.



## Mission statement

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

The EDPS is responsible for:

- monitoring and ensuring that the provisions of Regulation (EC) No 45/2001 <sup>(1)</sup>, 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 Community 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.

---

<sup>(1)</sup> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).



## Foreword



I have the pleasure to submit a fifth 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 2008 as the fourth 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.

This report also concludes the first EDPS mandate and provides an opportunity to take stock of developments since the start. The independent control as provided for in Article 286 of the EC Treaty and confirmed as a general principle in Article 8(3) of the Charter of Fundamental Rights of the European Union, as well as in the Treaty of Lisbon, is a crucial condition for an effective protection of personal data in practice.

Fundamental rights and freedoms, such as the respect for private life and protection of personal data, can only become a reality if they are delivered in practice, both in the information systems of Community institutions and bodies, and in the adoption of new rules and policies that have an impact on the protection of personal data. The activities of the EDPS provide useful incentives in both areas.

This report shows that great progress has been made both in supervision and in consultation. Compliance with data protection rules and principles is developing, but there are still great challenges ahead. Perhaps most remarkable is the scope at which the EDPS is performing, in comparison to its virtual non-existence at the start.

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.

I also want to express special thanks — firstly to Joaquín Bayo Delgado who has been an excellent Assistant Supervisor, with great dedication, practical sense and good team spirit, and secondly to our members of staff. The qualities that we enjoyed in the staff are outstanding and have continued to contribute greatly to our effectiveness.

Finally, it is also appropriate at this stage to thank the European Parliament and the Council for their confidence in reappointing me for a second term and for appointing Giovanni Buttarelli as the new Assistant Supervisor.

Peter Hustinx  
*European Data Protection Supervisor*



# 1. Balance and perspectives

## 1.1. General overview of 2008

The activities of the European Data Protection Supervisor (EDPS) in 2008 have been based on the same overall strategy as before, but continued to grow both in scale and in scope. The capacity of the EDPS to act both effectively and efficiently has also been improved.

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

- a ‘supervisory’ role, to monitor and ensure that 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.

<sup>(2)</sup> See the 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: [http://europa.eu/agencies/community\\_agencies/index\\_en.htm](http://europa.eu/agencies/community_agencies/index_en.htm)

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 2008 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 will be discussed in Chapter 6.

The fundamental right to respect for private life and protection of personal data, as provided for in the Charter of Fundamental Rights of the European Union and in the Treaty of Lisbon, are increasingly relevant both for individuals and institutions, and for society as a whole. In a world that more and more depends on the use of information and communication technologies, these rights are designed to ensure that every individual can participate without fear that his or her private life and personal data are unlawfully compromised. Respect for privacy and protection of personal data are therefore also intended to generate trust and confidence in advanced technological environments.

However, this does not happen by itself and with legal provisions alone. It requires a systematic implementation of privacy safeguards in practice, a translation of general rules and principles in concrete technical and organisational arrangements that enable the right safeguards to be delivered in everyday reality. This also assumes that those responsible for this implementation and translation process are sufficiently aware of the need to do so and are held accountable for reaching the required results at the right time.

With this in mind, the EDPS is working to promote a 'data protection culture' within institutions and bodies, where compliance with data protection rules and principles are seen as a matter of course. As a supervisor, the EDPS aims to stimulate responsibility and accountability, by measuring progress and setting targets where necessary, but without being unduly prescriptive. The EDPS is also working to integrate respect for data protection principles in EU legislation and policies, whenever relevant. As an advisor, the EDPS aims to highlight where proposals for legislation and new policies have already dealt with these principles in an adequate way and where they should be improved in order to meet the requirements. In cooperation with national supervisory authorities and supervisory bodies in the 'third pillar', the EDPS is working to improve consistency in the protection of personal data in the EU as a whole.

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 2008, with more opinions issued than ever before. While most institutions and bodies are making good progress in developing compliance with Regulation (EC) No 45/2001, the emphasis of supervision is now shifting to monitoring the implementation of recommendations in prior checking and to improving the level of compliance in agencies. The EDPS has also completed a first series of inspections on the spot in different institutions and bodies to measure compliance in practice. The total number of complaints continued to increase, with less admissible complaints than before, but more complexity on the whole. Further work was also done in consultation about administrative measures and in development of horizontal guidance. The network of internal data protection officers has reached its full scope and continues to be an essential basis for effective supervision (see Chapter 2).

The EDPS further improved his performance in consultation in 2008 and submitted opinions on an increasing number of substantial proposals for legislation. He widened the scope of his interventions to a greater variety of policy areas, and to all stages of the legislative procedure, i.e. from the earliest phases of policy making, by reacting to Green Papers or requests for informal consultation, until discussions in Parliament and Council at different stages, including the final stage of conciliation. The majority of the EDPS's opinions continued to concern issues related to the area of freedom, security and justice, but other policy areas, such as e-privacy, public access to documents and cross-border healthcare, were also quite prominent. The EDPS furthermore published a policy paper on EU research and technological development, and was involved in an increasing number of court interventions (see Chapter 3).

Cooperation with national supervisory authorities continued to focus on the role of the Article 29 Working Party, which resulted in the adoption of a new work programme with four main strategic themes and several good results in its first year of operation. The EDPS also continued to put emphasis on the coordinated supervision of Eurodac, both for its own sake and in view of similar large-scale information systems expected in the near future. The need for close cooperation was very clear in relation to third pillar matters. Finally, cooperation in other international forums continued to attract attention, including the 'London initiative' on raising awareness of data protection and making it more effective (see Chapter 4).

Information and communication are not only important instruments for visibility, but also essential conditions for the EDPS to be effective in supervision, consultation and cooperation. This is why much attention was devoted throughout the year to the improvement of existing services, which resulted in good progress, especially on the EDPS's website in terms of content and accessibility, while further improvements are in the pipeline (see Chapter 5).

The management of human, financial and other resources of the EDPS has moved a long way from the building of a new institution in the first years



of operation, through consolidation and increasing scale, to a situation where step-by-step improvements have allowed for continued stability and for increasing effectiveness and efficiency in different areas (see Chapter 6).

## 1.2. Results in 2008

The annual report 2007 mentioned that the following main objectives had been selected for 2008. Most of these objectives have been fully or partially realised.

### • **Support of DPO network**

The EDPS continued to give strong support to data protection officers (DPOs) and encouraged a further exchange of expertise and best practices among them. Particular attention was given to DPOs of recently established agencies, inter alia, at a special meeting to discuss issues for new agencies and to brief DPOs on recent developments.

### • **Role of prior checking**

A record number of prior-checking opinions were issued, with still some work ahead to finish prior checking of existing processing operations for most institutions and bodies. More emphasis was put on the implementation of recommendations. Results of prior checks and this follow-up were shared with DPOs and other relevant parties.

### • **Horizontal guidance**

Guidance on relevant issues common to most institutions and bodies (e.g. recruitment of staff, processing of health-related data) was developed, at first to facilitate prior checking for agencies. This guidance will soon be made available for all interested parties. A seminar was organised in December 2008 to share developments in supervision with other EU stakeholders.

### • **Measuring compliance**

The EDPS continued to measure compliance with Regulation (EC) No 45/2001 by all institutions and bodies, and will report on progress made by mid-2009. In addition to this general survey, a first series of inspections was held in different institutions and bodies to verify compliance on specific issues. A general inspection policy will soon be published at the EDPS's website.

### • **Large-scale systems**

The EDPS has continued to develop a coordinated supervision of Eurodac together with national supervisory authorities, and to implement the work programme adopted for this purpose. The results of these joint activities will be available in the course of 2009. The EDPS has also made first steps with regard to other large scale systems, such as SIS II and VIS.

### • **Opinions on legislation**

The EDPS issued a record number of opinions or comments on proposals for new legislation or related documents, covering a wider area than ever before, and ensured adequate input from the first until the last phase of the legislative procedure. The systematic inventory of relevant priorities was followed up throughout the year and where necessary updated.

### • **Treaty of Lisbon**

The impact of the Lisbon Treaty has been closely analysed, but its entry into force depends on final ratification by a few Member States. The analysis highlighted that the treaty has a great potential impact, both for institutional and substantive reasons, with clear opportunities for improvement of data protection.

### • **On line information**

The information available on the EDPS's website has been improved, both by updating and developing its content, and by enhancing its accessibility. Further improvements are expected in the course of 2009, and will also include the electronic newsletter.

### • **Rules of procedure**

The preparation of rules of procedure, covering the different roles and activities of the EDPS, has made good progress, together with the development of internal case manuals for the most important activities. The results will be available on the EDPS's website in the course of 2009 with practical tools for interested parties.

### • **Resource management**

The management of financial and human resources was consolidated or further developed and other internal processes were enhanced. The functionality and efficiency of internal control functions were also improved.

### 1.3. Objectives in 2009

This section of the annual report has been used in previous years to also briefly look ahead. This time, there is reason to expect a mixture of continuity and change. The first year of a new EDPS mandate and a partly new composition of the institution is the right moment to take stock of the possible need for adjustments. This year will therefore be used for a strategic assessment of the roles and tasks of the EDPS and to set out main lines of development for the next four years. This reflection will coincide with other new elements in our external environment, such as the challenges coming from a new European legislature, a new European Commission, a possible entry into force of the Lisbon Treaty, other new long-term policies and frameworks, and their combined impact on data protection. The EDPS intends to take a clear position in this context and will report on conclusions in the next annual report.

The following main objectives have been selected for 2009, without prejudicing the outcome of this strategic reflection. The results achieved on them will also be reported next year.

- **Support of the DPO network**

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

- **Role of prior checking**

The EDPS intends to complete prior checking of existing processing operations for most institutions and bodies, and put increasing emphasis on the implementation of recommendations. Prior checking of processing operations common to most agencies will receive special attention.

- **Horizontal guidance**

The EDPS will continue to develop guidance on relevant issues common to most institutions and bodies, and make it generally available. Guidelines will be published on fund videosurveillance that will also help to focus attention to situations giving rise to specific risks.

- **Complaint handling**

The EDPS will publish a policy framework for the handling of complaints to inform all parties involved about relevant procedures, including criteria on whether or not to open an investigation on complaints presented to him.

- **Inspection policy**

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. Inspection policy guidelines on relevant procedures will be published.

- **Scope of consultation**

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.

- **Stockholm programme**

The EDPS intends to give special attention to the preparation of a new five-year policy programme for the area of freedom, security and justice, for adoption by the European Council at the end of 2009. The need for effective safeguards for data protection will be emphasised as a key condition.

- **Information activities**

The EDPS will further improve the quality and effectiveness of the online information tools (website and electronic newsletter) and will assess and where necessary update other information activities.

- **Rules of procedure**

The EDPS will adopt and publish rules of procedure, confirming or clarifying present practices as to 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 activities relating to financial and human resources, and enhance other internal work processes. Special attention will be given to the long-term recruitment of staff, the need for additional office space, and the development of a case management system.

## 2. Supervision

### 2.1. Introduction

The task of the European Data Protection Supervisor (EDPS) is to supervise in an independent manner processing of personal data carried out by Community institutions or bodies that either completely or partially falls 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 of processing operations has continued to be the main aspect of supervision during 2008, as a clear result of the notifications received after the so-called Spring 2007 exercise (see Sections 2.3.3 and 2.5.1). 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. The EDPS has prior checked existing processing operations, together with those being planned, in most relevant categories. The EDPS's 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 2008 as in previous years, there has been no need to order, warn or ban, as controllers have implemented the EDPS's recommendations or expressed the intention of doing so and are taking



Assistant Supervisor Joaquín Bayo Delgado,  
responsible of the Supervision team.

the necessary steps. The promptness of the responses differs from one case to another. The EDPS applies 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) (Article 24.1 of the regulation). Some institutions have coupled the DPO with an assistant or deputy DPO. The Commission has also appointed a DPO for the European Anti-fraud Office (OLAF, a directorate-general of the Commission) and a 'Data Protection Coordinator' (DPC) in each one of the other directorates-general (DGs), in order to coordinate all aspects of data protection in the DG.

For a number of years, the DPOs have met at regular intervals in order to share common experiences and discuss horizontal issues. This informal network has proved to be productive in terms of collaboration. This has continued during 2008.



Data Protection Officers during their 21th meeting in Brussels (26 June 2008).

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

The EDPS attended a part of each of the DPO meetings held in 2008: in February in Luxembourg (European Parliament), in June (Committee of the Regions and European Economic and Social Committee, Brussels) and in October (European Commission, Strasbourg). These meetings were good occasions 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 arising in the frame of the prior-checking work. Progress in the field of prior-checking notifications was reported to the DPOs at each meeting.

The meetings between the EDPS and the DPOs also provided the EDPS with the opportunity to update the DPOs on the Spring 2007 exercise and its follow-up, notably in the field of inspections (see Section 2.5.1 ‘Spring 2007 and beyond’).

The meetings were an occasion for some of the DPOs and the EDPS to share initiatives taken for European Data Protection Day (28 January). A presentation on the status of pilot projects in the context of prior checking was also made by the EDPS, along with a presentation on transfers of medical data to national courts, and a presentation on contractual clauses to be inserted in tender contracts between EU institutions and subcontractors of personal data.

A meeting was also held in June at the EDPS’s premises for the DPOs of EU agencies, to discuss specific substantive and procedural issues relating to these agencies. This was also the occasion to discuss the new procedure for *ex post* prior checks for agencies (see Section 2.3.2 on ‘Procedure’). A presentation by the EDPS’s staff was made at this occasion on the main procedures for which the EDPS has concluded that they fall outside the scope of Article 27 of the regulation and are therefore not subject to prior checking.

The working group on time limits for conservation of data, on blocking and on erasure met for three working meetings during 2008. The Assistant EDPS and two staff members participated at these meetings. Information technology (IT) experts

from the institutions participating at the meetings were invited to join the discussions and give their comments. Draft scenarios illustrating the main issues were also submitted to them for discussion. A working paper resulting from the discussions of the working group was drafted and shared with the DPOs for further consultation by IT departments.

## 2.3. Prior checks

### 2.3.1. Legal base

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

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

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

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

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

The criteria developed in the previous years <sup>(4)</sup> continued to be applied in the interpretation of this provision, both when deciding that a notification from a DPO was not subject to prior checking, and when advising on a consultation as to the need of prior checking (see also Section 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 includes the time — normally 7 to 10 calendar days, but when those days coincide with holiday periods, they are working days — given to the DPO of the institution or 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. To date, no such tacit opinion has ever arisen.

For *ex post* cases received before 1 September 2008, the month of August has neither been calculated for institutions and bodies, nor for the EDPS.

#### Procedure for *ex post* prior checks in agencies

The EDPS has launched a new procedure for *ex post* prior checks in the EU agencies. Since in many

<sup>(4)</sup> See Annual report 2005, Section 2.3.1.



Supervision team during a meeting.

cases standard procedures are the same in most EU agencies and are based on Commission decisions, the idea is to gather notifications on a similar theme and to adopt either a collective opinion (for various agencies) or a 'mini prior check' addressing only the specificities of an agency. To help the agencies fill in their notifications, the EDPS will submit a summary of main points and conclusions on the relevant theme based on previous prior-checking opinions (notably the Commission). The DPO will then submit an Article 27 notification with a cover note highlighting specific aspects *vis-à-vis* the position of the EDPS in this field (specificities of the processing within the agency, problematic issues, etc.). This procedure was launched in October 2008 with recruitment as a first theme.

### 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. All opinions are available on the website of the EDPS together with a summary of the case. The register is now published on the EDPS's website, so that the notifications are also available.

### 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.

A case manual guarantees, as in other areas, that the entire team works on the same basis and that

the EDPS's opinions are adopted after a complete analysis of all significant information. It provides a structure for opinions, based on accumulated practical experience and is continuously updated. It also includes a checklist.

A workflow system is in place to make sure that all recommendations in a particular case are followed up and, where applicable, that all enforcement decisions are complied with (see Section 2.3.8).

### 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 already underway were brought into conformity with the regulation within one year of that date (i.e. by 1 February 2002). The appointment of the EDPS and the Assistant EDPS entered into effect on 17 January 2004.

Prior checks involve 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 cannot 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 2004 and 2005, certain categories were identified in most institutions and bodies and found suitable for a more systematic supervision (medical and other files containing health related data, staff appraisal — including recruitment of future staff, disciplinary procedures, social services and e-monitoring). Since Spring 2007, those categories are no longer applicable for prioritisation and are 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. Prior-checking cases are increasingly not related to those areas, but also for example to operations allowing linkages between different data bases not provided for in legal instruments (Article 27(2)(c) of the regulation).

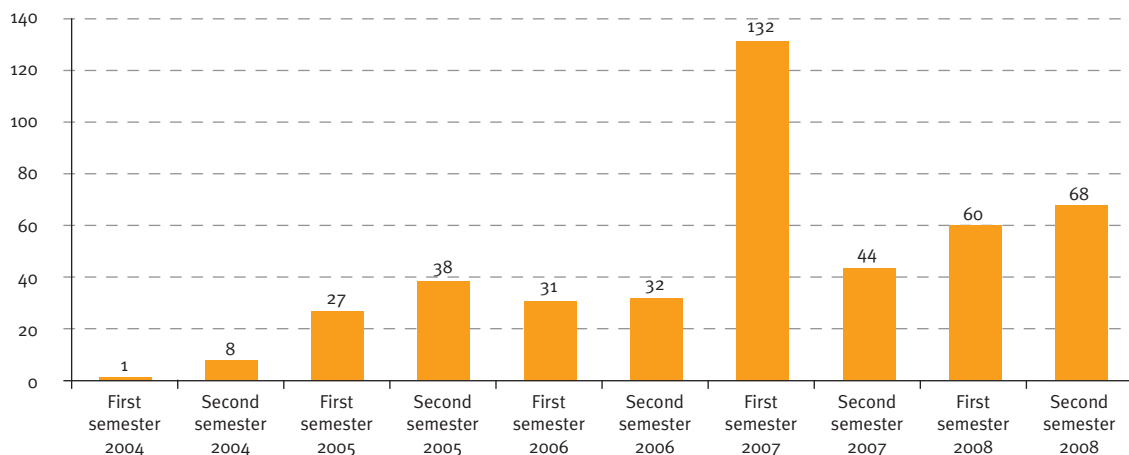
### 2.3.3. Quantitative analysis

#### Notifications for prior checking

As mentioned in previous annual reports, the EDPS has constantly encouraged DPOs to increase the number of prior checking notifications to the EDPS.

The deadline of Spring 2007 (see Annual report 2007) triggered institutions and bodies to increase their efforts towards a complete fulfilment of their notification obligation and resulted in a very meaningful increase of notifications. In 2008, there has been a clear slowdown of notifications, but as figures show (see the chart below), the number of issued opinions is higher than in 2007, as a direct effect of Spring 2007.

Notifications to the EDPS



### Opinions on prior-checking cases issued in 2008

In 2008, **105 opinions** <sup>(5)</sup> on prior-checking notifications were issued.

Council of the European Union	16 cases
European Commission	34 cases
European Central Bank (ECB)	1 case
Court of Justice of the European Communities	1 case
European Investment Bank (EIB)	2 cases
European Parliament	9 cases
Translation Centre for the Bodies of the European Union (CdT)	1 case
European Personnel Selection Office (EPSO) <sup>(1)</sup>	1 case
European Court of Auditors (ECA)	4 cases
Committee of the Regions (CoR)	1 case
European Economic and Social Committee (EESC)	3 cases
EESC / CoR	2 cases
European Ombudsman	1 case
Office for Harmonisation in the Internal Market (OHIM)	4 cases
European Anti-Fraud Office (OLAF)	4 cases
Community Plant Variety Office (CPVO)	2 cases
European Centre for the Development of Vocational Training (Cedefop)	3 cases
European Food Safety Authority (EFSA)	2 cases
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	5 cases
European Medicines Agency (EMA)	5 cases
European Maritime Safety Agency (EMSA)	3 cases
European Union Agency for Fundamental Rights (FRA)	1 case

<sup>(1)</sup> EPSO relies on the DPO of the European Commission.

Those 109 cases represent an increase of 8% of work in prior checking compared with 2007.

Out of the 109 prior checking cases (105 opinions), 18 were proper-prior checking cases, i.e. the institutions or bodies concerned (one each for ECA,

<sup>(5)</sup> The EDPS received 109 notifications but for practical reasons some cases were linked. This is why 109 notifications lead to 105 opinions.

Cedefop, EESC CoR, FRA and OHIM, two for the European Parliament, three for OLAF and four for the Council and the European Commission) followed the procedure involved for prior checking before implementing the processing operation.

Those 18 proper prior-checking cases resulted in 16 opinions as two cases for the European Parliament were respectively linked to FRA and the Council (FRA scientific committee members' selection and selection of the EDPS and Assistant Supervisor).

The other prior-checking opinions concerned the following subjects:

- flexitime;
- call for tenders (two cases);
- closed circuit television (CCTV) security system (see also Section 2.7);
- selection of candidates for the position of EDPS and Assistant Supervisor (Commission);
- linkages between data processed for different purposes not provided for in legislation (Article 27(2)(c) of the regulation) (interface flexitime PersonaGrata);
- identity and access control (two cases);
- Internet monitoring;
- pilot project on individual productivity monitoring;
- quality management system;
- administrative inquiries and disciplinary proceedings; and
- coordination of medical, psychosocial and administrative support (Compas) (see also Section 2.3.5).

The remaining opinions were *ex post* prior-checking cases.

In addition to the notifications on which an opinion was issued, the EDPS also dealt with 13 cases which were found not to be subject to prior checking. The EDPS is pleased to notice a decrease in the number of so-called 'non-prior checks'. This is certainly in part due to the Spring 2007 deadline which raised awareness among DPOs and led to a better assessment before sending notifications. The analysis of these 13 cases is developed in Section 2.3.7.

Nine notifications were withdrawn, including a special case from the EIB regarding the processing



operation on ‘politically exposed persons’ (its analysis is developed together with the ‘non-prior checks’ in Section 2.3.7). For the first time, the EDPS decided to suggest the withdrawal of some notifications. This was due to the fact that those notifications either concerned old processing operations about to be substituted by new ones or notifications that lacked sufficient information rendering it impossible to treat them with a correct understanding of the facts or the procedure.

The EDPS encourages the DPOs and the controllers to make notifications as clear as possible, which has the immediate effect of reducing the suspension time taken by the institution or body to reply to the EDPS’s requests for information. The EDPS intends to draft a documented notification form for all DPOs advising them and controllers on the exact information needed.

#### Analysis by institution and body

Following the Spring 2007 exercise, Community institutions and bodies have made progress in complying with the regulation. Most institutions and bodies have notified processing operations likely to present specific risks.

The European Commission has made important progress in this field, with a significant number of the notifications which have come from the Commission’s Joint Research Centre (JRC). The Council and the two Committees have made significant progress as well. The European Investment Bank and the European Central Bank have notified less but will have more occasions to do so because of new issues to be tackled.

With regard to agencies, Cedefop, EMCCD, EMEA and EMSA have been very active in notifying processing operations. Some other agencies have slowly started to notify processing operations. In 2009 there will no doubt be a marked increase in the number of notifications from the agencies. The EDPS has started to issue guidance on how to notify according to a new procedure for *ex post* prior checks from agencies based on guidelines issued by the EDPS, notably in the fields of recruitment and health data.

#### Analysis by category

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

Category one (medical files)	28 cases
Category two (staff appraisal)	53 cases
Category three (suspected offences)	6 cases
Category four (social services)	0 case
Category five (e-monitoring)	4 cases
Other areas	14 cases

**Category one** includes notably the medical file itself and its different contents, accident at work, sick leave, invalidity procedure, day-nurseries, sickness schemes, allowances procedures, radiation dosimetry and three various cases linked to health-related data. This category has significantly increased compared to the previous year. Among the 28 cases, 17 came from the different JRC sites. This increasing number has given the EDPS the opportunity to advise on the major procedures related to health data in the main institutions.

The major theme remains the **second category** relating to the evaluation of staff (53 opinions out of the 105). 23 cases were linked to recruitment (recruitment of officials, contractual and temporary agents, trainees, experts, scientific committee members, the EPDS and EDPS Assistant). Other cases related notably to evaluation, promotions, certification and attestation procedures, training, flexitime and early retirement.

Regarding the **third category** relating to offences and suspected offences, there has been a significant decrease of cases (six opinions as opposed to 18 in 2007). Only one opinion was issued on disciplinary procedures as most institutions had already notified those cases in previous years. Another opinion was issued relating to security investigations (see Section 2.3.4.), two opinions in the area of harassment and two other opinions in other matters.

Regarding the **fourth category** (social services), the EDPS did not receive any notifications, which is understandable as this category had already been

prior checked for the large institutions and most agencies are generally not in a position to offer that kind of service to their staff.

As regards the **fifth category** (e-monitoring), only four opinions were issued, as most of the notifications received related to processing of data for billing and traffic management and the EDPS therefore considered these as non-prior-checking cases due to the fact they do not present specific risks under Article 27. The opinion for the European Court of Auditors, however, needs to be underlined as it did concern monitoring of communications (Case 2008-284, see the analysis in Section 2.3.4).

Regarding the notifications which do not belong to any of these categories, the EDPS has continued to provide opinions in the following areas:

- tenders;
- access control system when a biometric matching tool system is used;
- closed-circuit television (CCTV) (one opinion which was a proper prior-checking case — see Section 2.7);
- linkage of databases (Case 2008-324 — PersonaGrata — Council — see Section 2.3.5.);
- various other matters, such as accreditations or testimony in justice.

### Compliance with deadlines

The four charts in Annex E of this report illustrate the time taken to process prior checking opinions by the EDPS and the Community institutions and bodies. They detail the number of days needed by the EDPS for drafting opinions, the number of extension days requested by the EDPS and the number of suspension days (time needed to receive information from the institutions and bodies).

*Number of days for drafting opinions by the EDPS:* There has been a decrease of more than two days of work compared to 2007 with an average of 55 days per opinion in 2008. This is a very satisfactory figure also considering the increase of numbers and the complexity of the notifications sent to the EDPS.

*Number of extension days for the EDPS* <sup>(6)</sup>: In nine cases the EDPS requested an extension period. Generally, although two months is possible for an extension (Article 27.4 of the regulation), one month is usually requested. In practice, however, all opinions were adopted within that month, the majority in significantly less time.

*Number of suspension days* <sup>(7)</sup>: There has been an increase in the number of suspension days between 2007 (with an average of 75 days per file) and 2008 (with an average of 122 days per file).

Taking into account that the average was 30 days per file in 2005 and 73 days in 2006, the EDPS is concerned by the lengthy periods needed by the institutions and bodies to provide further information. Indeed, some cases have been suspended for up to 524 days in order to receive further information. The EDPS finds this situation unacceptable and reminds the institutions and bodies of their obligation to cooperate with the EDPS to provide him with the requested information, according to Article 30 of the regulation.

*Average by institution and body:* for 2008, the charts show an alarming increase of suspension periods for nearly all institutions and bodies. With the exception of the European Parliament and EFSA, who have succeeded in decreasing their own average, all the other institutions and bodies have increased their suspension days very significantly. This is notably the case for the EIB, the Council, the Commission, the Court of Auditors, the Court of Justice and the agencies.

The EDPS recognises the fact that most of the suspension time is the controllers' responsibility. Nevertheless, DPOs should pay closer attention to those deadlines as they have the final responsibility for notification and further information, regardless of the fact that, for possible practical reasons, the requests may be addressed directly to controllers, with the DPOs in copy.

<sup>(6)</sup> According to Article 27.4, the EDPS may, where the complexity of the case so requires, decide to extend the two-month deadline within which he should adopt his opinion.

<sup>(7)</sup> Since mid-2006, this period includes the suspension for seven or ten days for comments and further information from the DPOs on the final draft. In *ex post* cases received before 1 September 2008, the month of August has not been calculated.

### Notifications for prior checking received before 1 January 2009 and pending notifications

By the end of 2008, 69 prior-checking cases were in process. Of these, one notification had been sent in 2006, 11 in 2007 and 55 notifications in 2008.

#### Analysis by institution and body

Parliament	7 cases
Council	6 cases
European Commission	33 cases
EESC and CoR	1 case
EESC	4 cases
CoR	3 cases
EIB	2 cases
ECA	2 cases
Court of Justice	1 case
Cedefop	1 case
CPVO	1 case
EFSA	1 case
EMEA	3 cases
ETF	1 case
FRA	2 cases
OHIM	1 case

#### Analysis by category

The number of notified prior-checking cases per category pending on 1 January 2009 was as follows:

Category one (medical files)	20 cases
Category two (staff appraisal)	26 cases
Category three (suspected offences)	4 cases
Category four (social services)	0 case
Category five (e-monitoring)	3 cases
Other areas	16 cases

### 2.3.4. Main issues in ex post prior-check cases

#### Health-related data

The EDPS issued various opinions on the processing of personal data in the field of absences for medical reasons (illness or accident). The EDPS

notably recommended that the data collected by the medical service of the European Parliament in order to justify an absence on medical grounds can only be used for other purposes (notably preventive purposes) with the free and informed consent of the data subject (Case 2007-688). The EDPS also considered in this case that the data could not be kept for longer than 12 years concerning persons who had since left the institution.

The EDPS also prior checked the processing of personal data relating to absences due to medical reasons at the Council in Joint Cases 2008-271 and 2008-283. Recommendations also mainly concerned the conservation of the data by the medical service controlling absences (*médecin contrôleur* in French) for 30 years and invited the service to reconsider this conservation period in the light of the purposes of the processing operation.

The EDPS issued a prior-checking opinion on the PowerLab software used by the Joint Research Centre (JRC) of the European Commission (Case 2007-649).

PowerLab is a software environment used for the management of the work cycle of clinical and radio-toxicological laboratories at the JRC. It is applied in relation to laboratory tests needed during pre-employment, periodic and other occupational risks related medical visits. It also includes production and/or storage of the respective test reports.



Community institutions and agencies process health-related data.

The main recommendations provided in the PowerLab prior-checking opinion related to:

- the necessity to comply with the professional secrecy obligation by all laboratory staff;
- the obligation not to use the data received for any further purposes than the one for which they were transmitted; and
- the need to provide complete information.

### Journalist's accreditation

The EDPS issued a prior-check opinion regarding the accreditation of journalists who attend European Council meetings (Case 2004-259). The purpose of the processing is to enable the Council's Security Office to conduct a security assessment of members of the press participating at summits. Those registered may, if necessary, receive a badge granting them access to the security perimeter established around the building where the summit takes place.

The management of information concerning journalists for the purpose of security check is done by collecting the information from a form available on a secure site (HTTPS) of the Council's intranet.

The system administrator then automatically creates lists of requests for 'screening', which are sent to the various security services (Belgian National Security Authority — NSA, or Presidency NSA).

The lists created for this purpose contain the name, surname, date of birth and nationality of the person. The results are communicated by NSAs to the responsible persons of the Security Office, first by telephone (for the sake of efficiency), then by official mail. They are limited to a 'positive' or 'negative' screening. However, according to the Decision of the Council's Secretary General No 198/03, the director of the Council's Security Office may exceptionally decide otherwise during the summit (e.g. in cases of inappropriate behaviour).

The initial conservation period is five years, but the Council raised the possibility of keeping the data for up to 30 years. In this respect, the EDPS recommended that a proportional conservation period be maintained, having regard to the purpose of processing. The EDPS also requested that the reference in the information notice saying that 'It is important to note that applicants provide data on a voluntary basis and that no one is obliged to give' is not included since, in many cases, journalists request accreditation in the context of their work environment and, therefore, the value of their consent in the terms of Article 2(h) of the regulation can be questioned.

A prior-check opinion was also adopted on the accreditation of external firms (Case 2007-046). The EDPS reached similar conclusions.

The EDPS issued an opinion (Case 2007-0349) on a notification for prior checking related to the processing of personal data that the Informatics DG of the European Commission carries out to operate the Identity Management Service (IMS).

The IMS is a service primarily used to manage user populations and their rights in the context of information services. In particular, IMS facilitates the authentication and access control of users to different European Commission information services, which are managed by different directorates-general. In doing so, IMS customises user



Accreditation of journalists and external firms for access to Council summits has been prior checked by the EDPS Identity Management Service

interfaces according to the user's individual characteristics. IMS is used for Commission staff as well as for personnel of other organisations and members of the public.

The EDPS's opinion concluded that the Commission had substantially complied with Regulation (EC) No 45/2001. Nevertheless, the EDPS made recommendations regarding the lawfulness of the processing, and suggested the need to obtain users' consent to process data processed through IMS for customisation purposes (interactively and on screen, for example, using the technique of a 'pop up' window). The EDPS also suggested shortening the data retention deadlines for log files in accordance with Article 37(2) of the regulation. The EDPS recognised that IMS is set up in a way that it regularly and automatically updates staff related information obtained through human resources databases and, therefore, ensures the accuracy of the data of staff members. However, a similar system did not appear

to exist regarding information of outside users. Such users may have been registered by third parties, such as their employers, with the enhanced risk for information to be inaccurate. The EDPS therefore underlined that it is important for IMS to put in place a system that ensures the accuracy of personal information of non-Commission staff members who have been registered in IMS by third parties, such as their employers.

#### **Access control**

The EDPS released a prior-checking opinion on the setting up of an access control system which scans the iris of the European Central Bank (ECB) staff members, as well as external individuals accessing highly secured areas within the institution (Case 2007-501). The system works together with a pre-existing access control system based on a contactless badge.

Although directly applicable only to the ECB, the EDPS's opinion served to give relevant guidance



Targeted impact assessments, evaluating the reasons that justify iris scanning and whether other, less privacy intrusive alternatives are feasible, are necessary.

more broadly as to the appropriate features of a privacy-compliant biometric system. In particular, the EDPS recommended that the ECB carry out an impact assessment reconsidering the decision taken in terms of technological choices. Indeed, given the highly sensitive nature of biometric data, the execution of a targeted impact assessment evaluating the reasons that justify the use of a biometric system is essential before the setting up of such a technique.

The EDPS also called upon the ECB to consider the implementation, in due time, of a 'one to one' search mode system where biometric data would be stored in chips rather than in a central database as with the current system. Furthermore, as biometric systems are neither accessible to all nor completely accurate, readily available fallback procedures should be implemented. Such procedures would respect the dignity of persons who could not be enrolled or could have been wrongly identified, and avoid transferring the burden of the system imperfections onto them.

In addition to the above, the EDPS recommended that the ECB enact a legal instrument providing the legal basis for the processing operations in order to set up an access control system based on the use of biometrics.

### **Recruitment**

Recruitment is a common processing operation in all institutions and bodies for obvious reasons. Many notifications were received by the EDPS in this field in 2008.

The EDPS carried out extensive prior checks on the recruitment procedures in the Joint Research Centres (JRC) of the European Commission. These procedures concerned:

- grant holders (Case 2008-138);
- interim staff (Case 2008-139);
- officials (Case 2008-140);
- contract agents (Case 2008-142);
- trainees (Case 2008-136).

In these opinions, the EDPS underlined the issue of the collection of certificates of good conduct

in the recruitment procedure and requested that the European Commission carry out a case-by-case analysis of the content of police record / criminal record / certificate of good conduct, so as to collect only relevant data in the light of the Staff Regulation requirements. The EDPS also encouraged the controller to find a system whereby information about crimes that have expired be deleted.

The following recruitment procedures at the European Parliament were notified to the EDPS:

- recruitment and transfers of officials (Case 2004-207);
- temporary agents (Case 2007-323);
- contractual agents (Case 2007-384).

Similar recommendations were made concerning the conservation of the extract of the police record / criminal record. The EDPS also recommended that, in the application forms, the mention of whether the candidate has been previously convicted be removed.

The European Ombudsman also notified the recruitment procedures for officials, temporary staff and contractual agents (Case 2007-405).

Similarly the Council notified the recruitment procedure for officials and other agents (Case 2007-194). A recommendation was also made on the conservation of the criminal record after the end of the recruitment procedure.

As mentioned in Section 2.3.2., the EDPS launched a new procedure for *ex post* notifications relating to processing activities on recruitment in the agencies. This has led to the establishment of guidelines on the processing of personal data in recruitment procedures and will lead to many notifications in this area. A few agencies have nevertheless already submitted notifications in the field of recruitment, notably EMEA (Case 2007-422), OHIM (Selection of managers – Case 2008-435), EMSA (recruitment of permanent staff, temporary agents and contractual agents – Case 2007-566, and recruitment of trainees — Case 2008-384), and the EMCDDA (Case 2008-157).

### Expert database

The EDPS received a notification concerning EFSA's expert database (Case 2008-455). This database contains professional data of external scientific experts who may be called upon to carry out advisory work for EFSA (and for national authorities in member states with a similar mandate to EFSA). Candidates apply on-line to be included in the database. EFSA then screens the applications to ensure that only those applicants who meet the eligibility criteria are included in the database.

The recommendations of the EDPS included, most importantly, the fact that end-users' attention should be specifically called to the limited nature of the validity check that EFSA carries out, suggesting that they use the database as a pool of applications, rather than as a pool of experts whose skills and reliability have already been carefully checked by EFSA in each case. The EDPS also recommended that automatic reminders should be sent to experts who failed to update their profiles (or confirm their old profiles) with a warning that failure to respond (after a number of reminders) would entail the automatic deletion of their profiles.

### Staff evaluation

In the field of staff evaluation, the EDPS adopted an opinion on the notification for prior checking received from the Data Protection Officer of the European Parliament regarding the Skills database (Case 2008-192).

This database contains career data on staff covering professional experience in and before joining the European Parliament. The Skills database is a processing operation that facilitates human resources management in mobility, careers advice, specialised staff search, filling vacant posts and planning competitions. The legal basis of this processing activity is Rule 197(2) of the European Parliament's Rules of Procedure, which foresees a power of organisation of the services of the institution. Given the general character of this legal basis, the EDPS recommended the adoption by the appropriate authority in the European Parliament of a decision stipulating the characteristics, definition and guarantees of the Skills

database, in order to ensure transparency and legal certainty.

Another prior-checking opinion relating to staff evaluation concerned the system of internal quality checks during which the work products of OHIM's trademark examiners are reviewed and the results are reported in a database created for this purpose (Case 2008-437). The primary purpose of these systematic checks is to improve the overall quality of OHIM's work products. However, the results of the checks are also used to evaluate the quality of work of each examiner and inform management of decisions regarding measures that may individually affect the examiners, such as performance appraisals, promotion, contract renewals, disciplinary measures, or training.

In his opinion, the EDPS recommended the adoption of a clear and formal internal decision to strengthen the legal basis of the operation and provide much needed clarity and certainty to staff members. This decision should clearly describe the system of the *ex-ante* quality checks, including their intended purpose, and provide for appropriate data protection safeguards.

The EDPS also emphasised that all possible efforts should be made to improve the level of accuracy, reliability, and consistency of the data. In any event, data included in the database should only be used as one of several factors to be considered in the decision-making process. Whenever data stored in the database are used for purposes which may individually affect staff members, the staff members must also be heard and given the opportunity to put forward their positions.

### Security investigations

The EDPS issued an opinion on security investigations at the European Commission (Case 2007-736). The security directorate — administrative requisitioning is competent to take certain measures against criminal or unlawful acts as concerns buildings occupied by the Commission, persons working within these buildings or who have access to them, along with any other acts which may prejudice the institution. This includes the storing of any elements of proof, searches to collect such elements, hearing

the declarations of plaintiffs, witnesses or, if need be, of the persons responsible for such acts.

The EDPS examined the processing of the data in the procedures of security investigations and requested that the service examine the proportionality of the activities carried out. In this respect, the investigations must be proportionate not only to general purpose of the processing activity, but also to the purpose of the specific processing operation. The EDPS also highlighted the necessity of affording adequate guarantees to ensure the protection of the data and recommended the adoption of a specific protocol to be respected in the frame of forensic searches. As concerns the transfer of data to third countries and international organisations, the EDPS recommended that, in those cases in which the transfer could only be justified on the basis of Article 9(7), a register be established containing information notably on the purposes of the transfer, the persons concerned, the right of access, the legal basis and the lawfulness of the transfer, the recipient of the data, and an indication of the conservation period of the data by the recipient.

The EDPS also highlighted the fact that the right of access to personal data must be established as a principle and that any exceptions to this right must therefore be applied restrictively. The EDPS accepted on this basis that Article 20(1)(c) of the regulation could serve to protect the interests of whistleblowers.

### **Procedure against harassment**

The EDPS issued an opinion on the informal procedure established at the European Commission against sexual and psychological harassment (Case 2008-062).

The EDPS notably underlined that the right of access and rectification, as established by Articles 13 and 14 of the regulation, should also apply to the personal notes of the confidential counsellor. The EDPS also recommended that the right of access to the file on an alleged harassment is also applied as regards third persons if these files contain personal data on him/her. This could be the case of persons considered as alleged 'harassers' or witnesses. The information contained in these files could be accessed directly by the person concerned

or indirectly (notably via the EDPS). Limitations to this right of access can be applied on the basis of Article 20 of the regulation, notably to protect the rights of others or if this access could prove harmful to the undergoing investigation.

### **Coordination of cases by OLAF**

The EDPS adopted an opinion on the processing of personal data by OLAF when it opens a coordination case (Case 2007-699). These are cases that could be the subject of OLAF external investigations, but where OLAF's role is to contribute to investigations being carried out by other national or Community services by, among other things, facilitating the gathering and exchange of information and ensuring operational synergy among the relevant national and Community services. The main investigative input is provided by other authorities. OLAF's role includes facilitating contacts and encouraging the responsible authorities to work together. The type of personal information processed by OLAF in these cases includes identification, professional data and information concerning activities related to matters which are the subject of coordination.

In his opinion, the EDPS asked OLAF to ensure that individuals whose data are processed by the office are informed of the data processing that takes place in the context of coordination cases. This could take the form of information provided by the relevant national authorities, including in their privacy statement addressed to data subjects a paragraph informing them of the possibility for their personal data to be transferred to OLAF for coordination purposes. Because individuals will have been informed of the transfer of their personal data to OLAF by the relevant national authorities, it would not be necessary for OLAF to provide such information again. The opinion also suggested some amendments to the privacy statement and asked OLAF to conduct a preliminary evaluation of the necessity of the 20 years conservation period *vis-à-vis* the purpose of such conservation.

### **Authorisation to testify in justice**

The EDPS has prior checked the procedure established by the European Commission in order to



respect the provisions of the Staff Regulations on the authorisation to testify in justice. According to Article 19 of the Staff Regulations, ‘An official shall not, without permission from the appointing authority, disclose on any grounds whatever, in any legal proceedings information of which he has knowledge by reason of his duties. Permission shall be refused only where the interests of the Communities so require and such refusal would not entail criminal consequences as far as the official is concerned. An official shall continue to be bound by this obligation after leaving the service’.

In his opinion, the EDPS made recommendations on the right of defence in the sense that the official must be invited to express himself prior to the decision of the appointing authority providing there are no restrictions to this right under Article 20(1) of Regulation (EC) No 45/2001.

### 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 of Regulation (EC) No 45/2001. In parallel with the handling of *ex post* prior checking, 18 cases of ‘proper’<sup>(8)</sup> prior checking were notified to the EDPS in 2008. This resulted in 16 EDPS opinions (see Section 2.3.3).

#### Selection procedures

The EDPS received a notification for prior checking from the European Union Agency for Fundamental Rights (FRA), relating to the processing of personal data in the selection procedure of members of the agency’s scientific committee. A subsequent notification was received from the European Parliament on the processing of personal data in the frame of the next step of this selection procedure at the Parliament’s LIBE Committee (Civil liberties, Justice and Home Affairs Committee).

Since both these notifications related to the same selection procedure, the EDPS issued one opinion

covering the entirety of the selection procedure (Cases 2008-179 and 2008-202).

The EDPS’s analysis primarily led to recommendations in the field of information of the data subjects. Indeed, although the procedure had already been launched, the candidates had not been informed that the data which they had submitted during the selection procedure (CV, motivation letters, etc.) would be made public as a consequence of the public procedure of the LIBE Committee sessions. According to Article 12 of the regulation, this information should be provided at the time of collection of the data or, at the latest, at the time when the data are first disclosed to a third party. Since this information was not provided in the call for expression of interest, the EDPS recommended that:

- the FRA inform all short-listed candidates, prior to the communication of their data to the LIBE Committee, that the data which have been submitted by them will be publicly available as a result of the public nature of the European Parliament sessions and that they have a right to object to the publication of their data;
- the FRA inform short-listed candidates of the procedures to exercise their right of access and of the right to have recourse to the EDPS.

The EDPS also recommended that this information be inserted in the FRA website so that it is accessible for the candidates who had not been short-listed. The EDPS furthermore considered that information on the processing of personal data should remain available on the FRA website at least until the end of the selection procedure.

The EDPS also prior checked<sup>(9)</sup> the processing of personal data involved in the selection procedure of the EDPS and Assistant EDPS. Two opinions were issued in this field, one relating to the procedure at the European Commission relating to the establishment of a short-list of candidates to be submitted to the Council and the European

<sup>(8)</sup> That is, cases concerning a processing operation not yet implemented.

<sup>(9)</sup> This happened under the responsibility of the Assistant EDPS not involved in the selection procedure.

Parliament (Case 2008-222) and another opinion on the procedure taking place at the Council and Parliament (Cases 2008-280 and 2008-292).

Concerning the first part of the procedure, the EDPS highlighted the fact that, at all stages of the procedure, the recipients to whom the data are transferred are reminded that they can only process the data for the purposes of the selection of candidates to be short-listed for the position of EDPS and Assistant Supervisor. Furthermore, the EDPS noted that the CV-Online application was being used and that this tool requested information on the personal number of persons working within the EU institutions. Taking into account the fact that the CV-Online is a standard IT tool used in the Commission for all selection procedures of senior management, both external and internal, and that, in some instances, the personal number could prove to be necessary for the selection phase of these other procedures, the EDPS recommended that the Commission clearly indicate in the page of instructions to candidates that the reference to the personal number in the CV-Online application form is fully optional and that candidates are not required to fill it out. Particular emphasis was also made on the importance of informing the candidates that their data would be made public, due to the public nature of the LIBE Committee sessions.

Regarding the next part of the procedure taking place at the European Parliament and the Council, the EDPS issued a separate opinion. This opinion highlighted the importance of providing adequate information on the processing of the personal data to the short-listed candidates within both institutions.

#### **Individual monitoring/pilot project**

A prior-check notification was submitted to the EDPS on a pilot project at the Council on individual productivity monitoring (Case 2008-436). In view of providing heads of language units and individual members of staff with individual performance indicators, the proposed tool should enable individual members of staff to monitor their own production and the head of the data subject's unit to monitor the production of any

given member of the unit, and to monitor the production of all members of the unit in one simple operation.

The processing operation was submitted for prior checking, firstly because of the fact that the output of the pilot project would be used by the head of the data subject's unit as one element in the assessment of the production of each member of staff, notably during the reporting exercise, and the processing of data was therefore intended to evaluate the efficiency of staff members (Article 27(2)(b)). Secondly, the processing involved links between two data bases which are not provided for by the national or Community legislation (Article 27(2)(c)).

The EDPS took the occasion of this prior check to remind the Council of the policy as concerns pilot projects. In principle, the project may not commence before the implementation of the recommendations made by the EDPS in his opinion. Furthermore, the end of a pilot project does not automatically trigger the full deployment of the system, so that it can be implemented right away. Indeed, it is necessary to analyse the results produced by the pilot phase before starting a full deployment of the system. The results of the pilot project must be communicated to the EDPS prior to the launch of the general project and the EDPS must be informed of any modifications in the general system that are likely to have an impact on the processing of personal data. The EDPS will subsequently analyse the results of the pilot project and any data protection implications prior to the launching of the general system. The EDPS underlined in his recommendations that, should that specific pilot project become a full fledged project at the term of the pilot project, a legal decision or instrument providing a specific legal basis for the processing of personal data should be adopted.

#### **Flexitime**

Another opinion based on Article 27(2)(c) of Regulation (EC) No 45/2001 was adopted regarding the interface between Flexitime and the PersonaGrata systems of the Council (Case 2008-324). The PersonaGrata system is a management

tool designed to organise work in the translation services of the Council. The purpose of the interface is to import data from the flexitime system into the PersonaGrata database thereby avoiding the duplication of data considered as equivalent between the two databases.

The EDPS considered that the recording of data was not equivalent as this category of data is specific to a Flexitime system. Moreover, the number of entries linked to absences in the Flexitime system was higher than those in the PersonaGrata system. Therefore, the various reasons of absence were presented to the users as one and only motive for absence in the PersonaGrata system. The EDPS underlined that the equivalence of data in both systems could help guarantee the respect of the data quality principle.

The EDPS also issued an opinion on the processing operations relating to the flexitime specific to the Enterprise and Industry DG at the European Commission <sup>(10)</sup> (Case 2008-111). In this processing operation, the Enterprise and Industry DG intended to implement a button interface in the staff PCs to collect presence data.

In his analysis, the EDPS considered that the purpose of the notified processing operation by the Enterprise and Industry ENTR did not fully meet the purpose of flexitime, as derived from the analysis of the time management system (TIM) of the European Commission. Indeed, in the notified case, if data were to be temporarily stored by the head of unit, this could lead to evaluation not foreseen by the TIM. The EDPS therefore opposed the sending of electronic mails to a functional mailbox of the heads of units. Having said this, the EDPS recognised that the idea to have a user-friendly interface to store timestamps into TIM, without the need to use the graphical user interface of Sysper2-TIM, could be welcomed.

### **E-monitoring**

The monitoring of the use of the Internet by the staff of an EU institution or body has given the EDPS the occasion to underline his preference

<sup>(10)</sup> The Time Management Module (TIM) integrating flexitime into the staff management tool (Sysper 2) at the European Commission had been the object of a previous prior check (2007-063).



Covert monitoring, where users are unaware that the monitoring of their Internet use is taking place, is not permissible.

for a preventive approach to the misuse of the Internet rather than a repressive one, and emphasise the need for proportionality in the means used (Case 2008-284).

In this respect, the EDPS notably concluded that, in the absence of an adequate suspicion, the monitoring of all the URLs visited by all the users is unnecessary and excessive. In order to detect misuse, the EDPS advised to make use of indicators (volume of data downloaded, time spent surfing, high number of failed attempts to access blocked sites etc) rather than monitoring URLs. The EDPS nevertheless conceded that, in certain specific circumstances, it may be necessary for the institution to monitor the URLs of specific individuals. This is the case when there is an adequate suspicion that a given user is engaged in behaviour against the institution (e.g. downloading paedophilic material) as well as when the length of URLs could indicate a possible attempt to engage in a URL attack.

### **Closed-circuit television system**

The EDPS adopted an opinion on the closed-circuit television system (CCTV system) operated by the European Anti-Fraud Office (OLAF) within its premises in Brussels for security purposes (Case 2007-634). This case is the first case among the EDPS's opinions involving video-surveillance. For more information on this case, please refer to Section 2.7.2.

### Identity and Access Control

The EDPS adopted an opinion on the OLAF identity and access control (Case 2007-635). The system is part of the security infrastructure that protects the OLAF premises and information and technology systems. The system is designed to control the identity and permit or deny access to persons entering and exiting from OLAF's premises outside working hours and special secure zones. To do so, OLAF uses a smartcard and fingerprint authentication. Users' biometrics data are stored only on the smartcard which cannot be used for any other purpose.

In the context of OLAF's access control, the EDPS interpreted the need-to-know principle as requesting that only the people who need special access should be enrolled in the system and therefore be fingerprinted. Therefore, the EDPS recommended that OLAF reassess and consider the possibility to restrain the list of people that will have to enrol their fingerprints, based on the real needs either to access OLAF outside normal office hours, or to access internal protected areas, or to use unguarded access points – staircases — to access the OLAF secure premises.

OLAF intended to keep the recorded data (or access control information) for no longer than one year for the purpose of investigating security incidents. The EDPS recognised that it may be necessary to keep an audit trail of the registering data for a period of time which allows reconstructing events during security related incidents and that, in the case of OLAF, it may not be practical to have a very short period. However the EDPS underlined that OLAF should develop a process of identifying and responding to incidents so that they are detected and reported as soon as possible after they have occurred. He also invited OLAF to reconsider the setting of its conservation period by reassessing the need to shorten this time by using the statistics of incidents.

The EDPS also issued an opinion related to the processing of personal information carried out by OLAF, to ensure that only authorised persons have access to OLAF's core information technology (IT) systems and to allow investigation of security

incidents (Core Business Information System — CBIS) (Case 2008-223). Authentication in CBIS is based on digital certificates and fingerprints. Certificates are stored on the personal OLAF badges (smartcards) of users and protected by a biometric match-on-card authentication scheme. Each user will have three fingerprint templates stored on his/her OLAF badge, which is a contact interface used by the CBIS IT authentication system.

In his opinion, the EDPS specifically analysed the respect of the data quality principle. To do so, he made a thorough analysis of the implementation of fall back procedures in the case of failure to enrol. Although the EDPS considered that the solution proposed by OLAF diminished the risk of failure to enrol, an impossibility to enrol could still exist and if such situation occurred, it would be discriminatory. Therefore, the EDPS suggested that OLAF should develop a workable alternative solution if and when a case of permanent impossibility to enrol occurs. Moreover, he also examined the way the false rejection rate is defined and recommended that OLAF establish a precise false rejection rate, which would reflect the security policy it has adopted.

### 2.3.6. Consultations on need for prior checking

During 2008, the number of consultations on the need for prior checking by the EDPS remained stable: 20 consultations in 2008 and 20 in 2007.

Several cases have been declared subject to prior checking such as:

- recruitment of interim staff;
- publication of the promotion points;
- traffic infringement;
- biometric data and access control.

Some processing operations have not yet been formally notified to the EDPS following his feedback on the need to prior check.

The processing operation relating to road infringement at the Council was considered as subject to

prior checking as it includes data on criminal convictions or on suspicions of criminal offences.

The processing operations about biometric data and access control were concluded to be prior checkable when biometric matching systems are used. Indeed, such systems present specific risks to the rights and freedoms of data subject. The EDPS's views are mainly based on the nature of biometric data which are highly sensitive, due to some inherent characteristics of this type of data. For example, biometric data change irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use. In addition to the highly sensitive nature of the data, the EDPS also notes that possibilities of inter-linkage and the state of play of technical tools may produce unexpected and/or undesirable results for data subjects.

The processing operation on the investigations of the Data Protection Officer (DPO) at the Court of Justice was not concluded to be prior checkable. Indeed, it did not aim to evaluate the conduct of a person or to evaluate his responsibility. In addition, the assessment by the DPO of a breach of the rules of Regulation (EC) No 45/2001 is a broader concept than suspected offences, offences or criminal convictions. The fact that data relating to suspected offences, offences or criminal convictions may appear occasionally does not change the scope of the processing operation.

The case related to the access to confidential documents was not considered as being subject to prior checking as the nature or the scope of the processing operation falls outside the scope of Article 27 of the regulation. Indeed, if data relating to health, suspected offences, offences, criminal convictions or security measures may appear in the confidential documents, the purpose of the processing operation is not to process such data but only to register the persons who access the documents.

### 2.3.7. Notifications not subject to prior checking or withdrawn

In 2008, the EDPS also dealt with 12 cases which were found not to be subject to prior checking

(9.91 % of the cases submitted to the EDPS). This conclusion was reached after a careful analysis of the notification. Nevertheless, this analysis led to some recommendations by the EDPS. Two of these cases related to the telecommunication area, two to access control, seven <sup>(11)</sup> to the area of personnel, and one to other areas such as Advanced Records System (ARES) and *Nomenclature commune* (Nomcom).

As concerns the seven cases related to the area of personnel, one of them dealt with time management <sup>(12)</sup>. It was considered non eligible for prior checking as this notification was linked to the master notification of Flexitime <sup>(13)</sup> and there were no substantial changes regarding the processing itself. The EDPS did however make some recommendations about the data retention period.

Regarding access control, one of those notifications <sup>(14)</sup> was submitted under Article 27(2) (a) of the regulation (a specific risk is present in processing operations of data relating to security measures). The EDPS has interpreted the notion of 'security measures' in Article 27(2)(a) as not relating to the physical protection of buildings and staff, but rather as the measures taken as regards individuals in the context of criminal (or administrative) procedures ('*mesures de sûreté*' in French).

The EDPS has also considered whether other aspects of the processing trigger the need for prior checking. In this respect, the use of the RFID technology is a relevant aspect. The EDPS considers that use of RFID, without any other additional element, does not present specific risks in the sense of Article 27(1). This does not mean however that best practices should not be

<sup>(11)</sup> EMCDDA legal entity and bank identification (2008-168), FRA processing operations in relation to salary payments (2008-396), OHIM appraisal procedure (2008-415 update of notification), Commission Staff management at JRD ITU in Karlsruhe (2008-151 the uses of the database are related to quite distinct processing operations, they have not been described in the notification with sufficient detail), Commission — JRC Karlsruhe — ZEUS flexitime (2008-486), Cedefop personal files (2008-197) and ombudsman Superviseo (2008-052 tool not for the purpose of evaluation).

<sup>(12)</sup> Commission — JRC Karlsruhe — ZEUS flexitime (2008-486)

<sup>(13)</sup> Commission — Sysper 2 Time Management (TIM) (2007-063)

<sup>(14)</sup> Cedefop (2008-195)

recommended to guarantee privacy and data protection. Nevertheless, recommendations were made about the exact purpose of the processing, the description of internal access control, information of data subjects, data retention period and technical security measures.

Among the 10 withdrawn cases, a specific case from the European Investment Bank (EIB) and related to 'politically exposed persons (PEP)' (Case 2007-543) needs to be underlined. The EDPS had originally been notified for prior checking regarding a procedure at the EIB on politically exposed persons set up to comply with Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. This notification was subsequently withdrawn since the manual 'PEP database' originally envisaged was not likely to be set up in the future. Alternative monitoring tools are being envisaged and these will be submitted to the EDPS for prior checking in due course.

Pending the adoption of alternative monitoring tools, current Chief Compliance Officer checks are taking place in view of ensuring compliance with Directive 2005/60/EC. The EDPS therefore made certain recommendations, notably concerning conservation periods and information to be provided to data subjects.

Regarding the conservation period, the EIB has established a 15 year conservation period in order to take into account, in addition to general time limitations for civil actions, possible requests for access from authorities worldwide in connection with terrorism and other serious crimes under the directive. The EDPS invited the EIB to reconsider the conservation period of 15 years in the light of actual requests for information by national authorities.

As concerns the obligation to inform data subjects in accordance with Articles 11 and 12 of the regulation, the EDPS recognised that providing information to each PEP could in some cases seriously disrupt and void the effectiveness of the EIB money laundering prevention activities under the directive. To this effect, the exemptions to the obligation to inform, as provided for

in Article 20(1)(a), (b) and (c) of the regulation, could be applied. Furthermore, considering that in many cases the EIB has no direct or contractual relationships with the individuals concerned, the exception provided for in Article 12(2) could also be applied. The EDPS was prepared to accept, as an alternative to individual information, a general information notice regarding data processing procedures relating to PEPs to be posted on the EIB website and published in EIB documentation.

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

When the EDPS delivers the prior-check opinion, a series of recommendations which must be taken into account in order to make the processing operation comply with the regulation are usually provided. Recommendations are also 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.

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

All prior checking cases have led to recommendations. As explained above (see Sections 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. The EDPS has now requested, in the formal letter sent with his opinion, that the institution or body concerned informs the EDPS of the measures taken to implement the recommendations within a period of three months. During 2008, the EDPS closed 36 cases, which represents nearly the same number of cases as in 2007. This figure should increase in 2009 as a lot of follow-up has been launched or reaffirmed.

### 2.3.9. Conclusions and the future

As in previous years, prior checks, especially *ex post* prior checks, have been a very important tool in the supervision of Community institutions and bodies.

Conclusions for 2008 can be summarised as follows.

- The year 2008 has been an intensive year of work, with 105 opinions issued, even more than in 2007 (90 opinions).
- This has been done with a decrease of days for drafting the opinions and a significant decrease of extension days needed.
- On the contrary, there has been an alarming increase of suspension days needed to receive information from controllers or data protection officers.
- A new procedure has been started for *ex post* prior checking of processing operations in agencies to facilitate both notifications and drafting of opinions, with a systematic approach by themes.
- Some meaningful issues have been addressed for the first time and included identity management service, access control with iris scanning or fingerprint authentication, security investigations, monitoring of the use of the Internet by staff, CCTV system, etc.

Future efforts will concentrate on the following points.

- The main institutions should complete their notifications in all fields coming under Article 27 of the regulation and agencies should progress significantly in complying with this obligation.
- The time needed to answer further requests for information from the EDPS has to be drastically reduced, mainly by drafting notifications and annexes in a satisfactory way.
- Some areas, such as video-surveillance, will see an important progress, applying the new policy limiting prior checking to systems departing from 'standard' practices foreseen in the guidelines (see Section 2.7).
- The follow-up of recommendations will continue both by receiving information from controllers (see Section 2.3.8) and through inspections (see Section 2.5).

## 2.4. Complaints

### 2.4.1. Introduction

Article 41(2) of Regulation (EC) No 45/2001 provides that the EDPS 'shall be responsible for monitoring and ensuring the application of the provisions of this regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body'. Part of this monitoring is carried out by the handling of complaints as provided for in Article 46(a) <sup>(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

<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'.

regulation <sup>(16)</sup>. Complaints can also be introduced by members of staff of the European institutions and agencies to whom the Staff Regulations apply, on the basis of Article 90(b) of the Staff regulation <sup>(17)</sup>.

Complaints are only admissible if they emanate from a natural person and relate to the breach of data protection rules by a Community 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 of the European Communities or the European Ombudsman (whether pending or not).

If the case is admissible, the EDPS proceeds to inquire about the case, as may be appropriate, notably by contacting the institution or 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 or body. He can also be granted access to any premises in which a controller or institution or body carries on 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;

<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.'

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

- 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>.

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

In 2008, the EDPS received 91 complaints. Of these, only 23 were declared admissible and further examined by the EDPS. Most of the other complaints did not concern personal data processing by a Community institution or body, but only related to processing at national level.

During 2008, 21 admissible complaints were resolved. A number of these are briefly examined below.

## 2.4.2. Cases declared admissible

### Collection or transfer of excessive data

The EDPS received a complaint from a staff member of the European Commission, concerning the request of the Commission to provide a complete Belgian tax statement of the spouse of a staff member in order to control the entitlement to the complementary health insurance cover (Case 2008-370). After investigation, the EDPS concluded that such a request was excessive and not in accordance with the principle of data adequacy laid down in Articles 4(1)(b) and 4(1)(c) of the regulation. Following the EDPS investigation, this practice has stopped and the Commission collects the data included in the Belgian tax statement only as far as the professional income is concerned and all other sources of income can be hidden.

Another complaint was received from a staff committee and various staff members of OHIM on the processing of personal data in a quality check system (Case 2008-0119). The complainants

<sup>(18)</sup> See Article 47(1) of Regulation (EC) No 45/2001.



requested that the EDPS look into the matter and confirm that:

- the linking of two possible databases for purposes other than historical, statistical or scientific does not affect individual staff members;
- the data gathered are adequate and relevant;
- the data gathered are effectively non-excessive, taking into account the numerous statistics on examiners' productivity already available for appraisal purposes;
- the data collected are accurate;
- the data are not kept for a period longer than necessary.

The EDPS considered that the complaint was admissible both for the representative of the staff committee and the staff members on the basis of article 33 and 90 of the Staff Regulations and that the EDPS was competent. He concluded that *a priori* there was no violation of the principle of data quality, nor of the rules as regards the conservation of the data.

However, the procedure under examination was intended to evaluate the quality of the work performed by examiners and notably forms part of the appraisal exercise. The EDPS therefore considered that the procedure qualified for prior checking. Prior checking should normally take place before a procedure is put into place, even if this procedure is only in a test phase and set up for a period of a few months. The setting up of the new quality check system without notification to the EDPS for prior checking would therefore be in breach of Regulation (EC) No 45/2001. On the basis of his powers as laid down in Article 47(1)(b) of the regulation, the EDPS invited the relevant body to notify the processing of personal data resulting from the quality check system, for prior checking under Article 27(1).

In another complaint, the complainant alleged that the names and surnames of all staff working for the European institutions in Luxembourg were transferred by the European Commission to the Luxembourg City bus services (Case 2008-421). The purpose was to issue a card for free bus services which do not display any names or surnames, but only a number. He alleged that this solution was not necessary, not proportional and it violated data protection principles.

The EDPS investigated the matter and noted that the Commission had sent a note of communication to its staff informing them before the processing operation had taken place of all necessary elements in accordance with Articles 11 and 12 of Regulation (EC) No 45/2001. Data subjects were given the possibility to accept or oppose to the transfer of their name and surname to Luxembourg City bus services. Consequently, in this context, the element of consent justified the lawfulness of the transfer in question according to Article 5(d) of the regulation. Moreover, the EDPS considered the Commission's initiative to issue free bus pass cards was a task carried out in the public interest in the light of the Staff Regulations that foresees the possibility for institutions to adopt measures of social service for the welfare of its staff. This additional element could therefore justify the lawfulness of the transfer under Article 5(a) of the regulation.

#### Access to data

An employee of the European Parliament submitted a complaint to the EDPS claiming that she was denied to exercise her right of access and rectification to her medical file by the sick leave management unit of the Parliament (Case 2007-681).

In his legal analysis, the EDPS gave *inter alia* a non-restrictive interpretation of Article 13 of Regulation (EC) No 45/2001 and held that the complainant did not only have the right of access to her medical file but also the right to obtain a copy or photocopy without any limitation in terms of copies of her own medical data. With regard to the right of rectification of her data, the EDPS stressed that, although it is impossible to rectify medical assessments, the complainant should have the right to keep her medical file up to date by adding other medical opinions. As to the complainant's request to transfer her medical file to the doctor appointed by her, the EDPS considered that the necessity of such transfer was demonstrated by her explicit consent, which also proved that it could not have prejudiced the data subject's legitimate interests.

The EDPS's decision on this complaint was of a particular interest for the European Parliament's trade union SFIE which sent an e-mail to the staff of the European Parliament citing the EDPS's recommendations.

Another complaint was received concerning an alleged violation of Article 13 of Regulation (EC) No 45/2001 by the European Commission and the European Personnel Selection Office (EPSO) as to the refusal of access to test results obtained in an open EPSO competition (Case 2007-0250). The EDPS was of the opinion that the complainant has a right of access to his results or marks obtained during the EPSO open competition pre-selection, written and oral tests, on the basis of Article 13 of the regulation. This right could be subject to certain limitations in terms of Article 20(1)(c) of the regulation. In particular, the names of the other applicants contained in complainant's comparative test results might need to be removed or masked, as well as — if necessary — the identification of the individual members of the selection board might need to be made impossible. Following the intervention of the EDPS, EPSO accepted to communicate the requested test results to the data subject and the case was closed.

An interesting complaint on access to 'non-existent' personal data was received from a former staff member of the European Commission (Case 2008-0438). The complainant complained about the fact that the Commission mentioned, in a letter addressed to him, a comparative study containing complainant's personal data. When asked to communicate the study, the Commission refused, arguing that the 'study' was never written and was based only on an oral consultation of an expert. After investigating the facts, the EDPS concluded that there was no evidence of the existence of the study and that, therefore, no personal data did exist and that there was no possibility to access them.

### **Processing of sensitive data**

The EDPS received a complaint from a former Commission employee claiming the improper processing of data relating to health in the frame of the management of the accident insurance (case 2007-0521). The complainant considered that

the special category of personal data in the terms of Article 10(1) of the regulation had been transferred to a third party without sufficient grounds for necessity according to Article 10(2)(b). In fact, the Commission transferred information related to the 'psychiatric expertise' of the data subject. After having analysed the facts, the EDPS concluded that the Commission had no grounds to disclose that particular expertise.

Another complaint was received from a Commission employee in relation to the processing of personal data related to his sex life (Case 2007-459). The complainant also complained about the leak of those data to third persons. After investigation, the EDPS concluded that:

- the complainant's personal data were processed without a legal basis;
- the complainant had not been provided with the necessary information concerning the processing (or with reasons justifying its deferral);
- the applicable security measures were not appropriate to the processing risks and the nature of the personal data.

Furthermore, the EDPS asked the relevant Commission's services to implement measures in order to prevent the breaches of Regulation (EC) No 45/2001 in the future. Following the EDPS's decision, the Commission committed to take appropriate action in order to comply with the provisions of the regulation.

A complaint was lodged against the European Commission in the context of a procedure for the attribution of parking places for staff with disabilities (Case 2007-611). A Commission employee complained that sensitive data related to his health were sent by e-mail to different third persons with no apparent reason. After evaluation of the facts, the EDPS concluded that there was a legal basis to forward the electronic mail to the other persons in order to be able to make a decision on the prolongation of the parking place, but that the medical data should have been deleted from the electronic mail sent to some of the recipients. The EDPS referred the matter to the controller and requested that the medical data be deleted by those recipients who received them unduly.

In another complaint, the alleged breach of data protection rights relates to actions taken on the basis of a request for special leave for a seriously ill spouse (Case 2007-602). The complainant claimed that the two medical certificates were given or at least shown by the head of personnel to the Appointing Authority (AIPN), in breach of Article 10(3) of the regulation.

After declaring the complaint admissible, the EDPS's decision focused on the fact that data relating to health were transmitted to the AIPN without the consent of the data subject and without being based on the EC Treaty or a legal act adopted on the basis of the treaties, in breach of Article 10(3) of the regulation.

Indeed, the implementing rules on leave provide that, in the frame of a request for a special leave of up to three days, a medical certificate must, in principle, be communicated to the leave manager. The rules do not provide that the medical certificate might be communicated to the AIPN. Indeed, the intervention of the AIPN is only explicitly foreseen in cases of chronic serious illness where the AIPN may grant extensions for up to three days. Furthermore, the implementing rules provide that when the person considers that the information contained in the certificate is confidential, the certificate may be communicated only to the medical service and the leave manager will only be notified of the basic information relating to the leave. As a consequence, this provision explicitly excludes the communication of confidential data to the leave manager and, therefore, *a fortiori* to the AIPN. In the absence of a medical service at the concerned body, the complainant communicated the medical certificate to the head of human resources, explicitly requesting confidentiality. The subsequent communication of such data to the AIPN did not therefore find grounds in the implementing rules.

The EDPS also raised the issue that since the procedure for the request of a special leave involves the processing of data relating to health, the procedure should be submitted to the EDPS for prior checking.

In another case, the complainant alleged that the processing of some of his data, within the framework

of the evaluation procedure in an agency, constituted a breach of Article 10 of the regulation (Case 2008-124). The data processed by his reporting officer for the appraisal exercise were related to the complainant's health (number of days on sick leave), to the professional activities of his spouse and to the fact that he was an active member of the staff committee.

As to his health-related data, the EDPS found that such data were relevant in as much as they were necessary to take into account the real period of time of work for his evaluation. As concerns the data related to the professional activities of the complainant's spouse, the EDPS pointed out that this information was irrelevant from a data protection point of view. With regard to his staff committee membership, the EDPS considered that such data are not covered by Article 10(1) of the regulation, which explicitly refers to the prohibition of the processing of personal data revealing trade-union membership and not staff committee membership. It was also pointed out that such data were relevant and not excessive for the purpose of the appraisal exercise since the time which is dedicated to this activity is part of the working hours, thus in accordance with Article 4(1) (c) of the regulation.

### **Right of rectification**

A complaint on the right of rectification of a civil servant of the European Commission was received by the EDPS (Case 2008-0353). The complainant sent several requests to different Commission services in order to rectify his personal data related to flexitime in Sysper2. The Commission did not react to those requests. Subsequent to the filing of a complaint with the EDPS, Personnel and Administration DG finally rectified the incorrect data in the relevant file.

### **Obligation to provide information**

A complaint was submitted by a data subject against the European Commission in the context of processing of data concerning accident insurance (Case 2007-0520). The complainant stated that data related to him, obtained from him and from third parties, were collected, stored and transferred to third parties without informing him accordingly (Articles 11 and 12 of the regulation).

The data subject also complained that the access was not granted to all his data processed by the Commission. Furthermore, the complainant maintained that he believed that the Commission gave a selective and tendentious presentation of his case, and he therefore wanted to exercise the right of rectification (Article 14 of the regulation).

After having evaluated the case, the EDPS concluded that the controller had not respected the obligations imposed by Articles 11 and 12 of the regulation and rejected the complaint on other grounds.

The EDPS received another complaint by a former staff member of the European Environment Agency (EEA) evoking an alleged breach of Regulation (EC) No 45/2001 by the agency, namely an unlawful and excessive transfer of the complainant's detailed financial data between two internal recipients within the agency (case 2007-0718).

The EDPS, after carrying out the necessary investigations, found that although the transfer of the complainant's financial data was necessary for the budgetary planning of a project, the agency had failed to inform the complainant of his rights regarding the transfer before it took place, in conformity with Article 12 of the regulation. In the EDPS's decision, it was therefore recommended that the agency should implement specific rules related to the transfers within the agency, the retention of data transferred and the information to be provided to the data subjects.

#### **Publication in the 2005 annual report — further update**

In July 2005, the EDPS received a complaint against OLAF which raised various issues under Regulation (EC) No 45/2001, 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).

In 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

the regulation, 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. This update was published in the 2007 annual report. Moreover, in the light of the decision of the Ombudsman on the second complaint, a corresponding note was added to the 2005 annual report as available at the EDPS's website.

As to the first complaint, the Ombudsman concluded in April 2008 that further inquiries into the complainant's allegations and claims would not be justified, and therefore closed the case. In a further remark, he recognised that in light of Article 46(a) and (b) of Regulation (EC) 45/2001, the EDPS indeed enjoys a certain margin of discretion as to which complaints he should investigate and conduct inquiries into. The Ombudsman also considered that it would be appropriate and very helpful to potential future complainants, if the EDPS were to announce, in a general policy document, what the criteria or the guidelines are that he intends to apply when exercising his discretion in opening inquiries and investigating complaints presented to him. This will be followed up in the context of the development of an internal manual on complaint handling and the subsequent publication of information on the main elements of the procedure, together with information on the admissibility of complaints, on the EDPS's website (see Section 2.4.5).

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

Out of the 91 complaints received in 2008, 68 were declared not admissible. The vast majority of these complaints did not concern personal data processing by a Community institution or body,

but exclusively related to processing at national level. Some of these complaints called 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 should a Member State fail to implement Directive 95/46/EC correctly.

### **Community institutions and bodies not directly concerned**

By way of example, the EDPS received two complaints concerning the processing of personal data of EC staff members, although the processing was not carried out by a Community institution or body, but by the trade unions operating within those institutions. One such example was a staff member complaining about having received political information to his office e-mail address from a trade union. In that case, the trade union used the list of all email addresses provided by the institution. However, the complaint was about a trade union acting under national law and having used that information (Case 2008-724). Another example concerned a disclosure of personal data to third parties by an EC staff trade union. In this case as well, the EDPS concluded that Regulation (EC) No 45/2001 was not applicable, the trade union concerned being a legal person under the national law (Case 2008-071). Therefore, the contact details of national data protection authorities were provided, along with an explanation of why the EDPS was not competent to deal with the case.

### **Violations not related to the processing of personal data**

The high number of inadmissible complaints also involved alleged violations by Community institutions and bodies, but whose subjects turned out to be outside the scope of Regulation (EC) No 45/2001. In fact, some complainants were trying to revise or annul individual decisions of the EC administration, arguing that those decisions contained some personal data and that their right to the rectification of personal data should be respected.

The EDPS declared such complaints inadmissible on the ground that, even if a decision of the EC administration contains personal data, this does not

imply that the EDPS is competent to investigate a complaint against such a decision. To be admissible, the complaint has to relate to the processing of personal data as such and not to the interpretation of personal data when an institution exercises its discretionary power.

### **The same facts are already examined by other bodies**

The EDPS usually declares a complaint inadmissible if the same matter (same factual circumstances) has already been examined by a court, the European Ombudsman or by similar administrative bodies. One such example was a staff member complaining about the failure to apply Regulation (EC) No 45/2001 in the context of an administrative inquiry conducted by a Community body. This administrative inquiry had been performed with a view to establishing facts related to a controversy about the alleged unauthorised access to the complainant's computer mailbox. The administrative inquiry was followed by disciplinary proceedings, still in process when the complaint was made. Furthermore, the complainant submitted a similar complaint to the European Ombudsman.

According to the EDPS, taking any position on the questions of failure to apply the regulation would be premature before the administration delivers its final conclusions on the matter in the disciplinary proceedings. The investigation of the case by the EDPS would also lead to the duplication of procedures with the European Ombudsman.

### **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 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 an inquiry carried out by the EDPS were forwarded to the Ombudsman so as to avoid duplication of investigations.

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

The EDPS has continued working on the development 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's website during 2009. This publication is expected to help potential complainants submit a complaint, whilst limiting the number of clearly inadmissible complaints and providing the EDPS with the more complete and more relevant information which should facilitate the complaint handling.

### **2.5. Inspection policy**

#### **2.5.1. 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

known as 'Spring 2007' as part of an effort to measure compliance with the regulation in the various institutions and agencies, and to take stock of the progress made so far.

The first part of the operation launched in 2007 took the form of letters addressed to directors of institutions and agencies in order to measure the level of compliance with the regulation. Four groups of questions were raised concerning: the status of the Data Protection Officer (DPO); the inventory of processing operations involving personal data; the inventory of those processing operations which fall under the scope of Article 27 of the regulation and further implementation of the regulation as such. This operation 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 or her duties. It has also encouraged agencies and institutions 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.

On the basis of the feedback received from the institutions and agencies, a general report on the level of compliance was drafted by the EDPS. This report was made public in May 2008 and was sent to all institutions and agencies.

As announced, the operation was 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. As concerns the latter, letters were sent out in October 2008 requesting further updates on the situation in the agencies and institutions. Additional questions were also raised on further implementation of the regulation, notably as concerns the exercise of the data subject's rights and the level of complaints lodged with the DPO. Replies to these requests were expected in December 2008 and will lead to a further report in the course of spring 2009.

### 2.5.2. Inspections

The EDPS has recently started further developing his inspection policy. The previous experience in conducting investigations in the framework of a complaint and the Spring 2007 exercise made it essential to systematise the EDPS's inspection activity under the powers vested in the supervisor in various articles of Regulation (EC) No 45/2001.

Inspections are a fundamental tool for the EDPS as a supervisory authority to monitor and ensure the application of the provisions in the regulation (Articles 41(2) and 46(c)). The extensive powers to access any information and personal data necessary for his inquiries and to obtain access to any premises where the controller or Community institution or body carries out its activity were designed to ensure that the EDPS can have efficient means to perform his public function (Article 47(2) of the regulation). Inspections can be triggered by a complaint or can be carried out at the EDPS's own initiative (Articles 46(a) and (b) of the regulation).

European institutions and bodies are required to cooperate with the EDPS in performing his duties and should provide the information and access requested (Article 30 of the regulation).

During inspections, the EDPS verifies facts and reality on the spot with a further goal to ensuring compliance with the regulation in Community institutions and bodies. In addition, inspections can largely contribute to raise awareness for data protection matters in the inspected institutions and an inspection can also support the work of the data protection officers.

In 2008, the EDPS defined the first comprehensive procedure for his inspection activities in the supervision area. It was a three-phase process:

- In the first phase, two rehearsal visits were carried out to test the EDPS's methodology on site.
- In the second phase, the EDPS refined its practical methodology.
- In the third phase, two inspections were carried out in European institutions which were selected in the framework of the Spring 2007 exercise.

### 'Rehearsal visits'

The general purpose of these on the site visits was twofold: apart from testing the EDPS's inspection methodology, they aimed at checking reality of complying with the regulation in certain selected domains. This therefore implied that the EDPS made recommendations in quite a few cases to improve the level of data protection at the visited services. In such cases, feedback was expected from the controllers within a set deadline.

#### *Council of the European Union*

In July 2008, three on-the-spot visits were carried out at the premises of the Council of the European Union (Case 2008-359). Apart from the aim to further refine the EDPS's practical methodology on inspections, the EDPS verified two personal data processing operations and held interviews at a directorate.

During the first visit, the EDPS verified certain items contained in the notification to the DPO (extracted from the DPO register) related to the processing of personal data in the framework of the establishment of rights at the time of taking up the duties (*fixation du droits* in French). Following the EDPS's recommendations issued following the visit, the controller has already informed the EDPS of the steps taken.

The next visit at the information and communication system directorate aimed at ascertaining what measures had been put in place by the controller to ensure that personal data processing operations would be notified to the DPO (Article 25 of the regulation). The EDPS will follow up the progress made in this area and requested feedback on the appointment of a contact person at the directorate for data protection matters and related to the status of notifications.

The third action covered a processing operation which had already been prior checked by the EDPS. The EDPS's staff members verified the personal data processing operations related to the trainee selection procedure (Case 2007-217) and the implementation of the EDPS's recommendations. The controller has already informed the EDPS on the

implementation of some of his recommendations made after the visit. A few issues are however still pending.

#### *OLAF*

In October 2008, the EDPS's staff members carried out an on the spot visit at the premises of OLAF with a view to further refining the EDPS's practical methodology for inspections. The objective was also to verify reality regarding the measures taken by OLAF to ensure the implementation of certain recommendations presented in the EDPS's prior-checking opinion on OLAF internal investigations (Case 2005-418).

The EDPS's visit (Case 2008-488) focused on a few items of significance from a data protection perspective, in particular the practice of identifying certain categories of data subjects in the 'persons' tab in the OLAF case management system (CMS). The EDPS's staff members also accessed selected OLAF cases in the CMS to see the information notices sent to data subjects, the practice on deferral of the obligation to inform and the personal data transfers in relation to the cases selected for the visit. In addition, the EDPS inquired about the foreseen notifications to the DPO of OLAF in cases where electronic mails or documents of personal nature were concerned in the context of OLAF protocol of standard operating procedures for conducting computer forensics investigations.

In providing the feedback to OLAF after the visit, the EDPS insisted on his earlier approach in the areas examined. The obligation to inform should be implemented and a note should be left in the file in case of deferring the information. Notices should be provided when a transfer of personal data takes place. The EDPS encouraged OLAF to address the practice of oral transfers. He urged OLAF to use the persons tab to identify data subjects in the CMS as a useful tool enabling the proper implementation of other obligations.

As the OLAF protocol on computer forensics is still a draft OLAF document, the EDPS encouraged the office to take the necessary steps to adopt the Protocol as an OLAF document and start applying it.

As a general observation, the EDPS encouraged OLAF to draft standard data protection statements and/or notices available for case handlers which they could add to the text of *ad hoc* documents. He further insisted on the need to adopt the necessary steps to put the whole data protection module in use to implement the obligations foreseen in Regulation (EC) No 45/2001.

#### **Refining practical methodology**

The two rehearsal visits enabled the EDPS to refine his internal inspection manual and draft the current version of the inspection policy guidelines.

The inspection manual provides a practical guide for EDPS's staff members working in the supervision area and who are members of an inspection team. It contains the description of the administrative procedure, tasks of inspectors, standard forms for producing inspection documents and security policy for inspections. It explains the purposes of those documents and gives useful tips in preparation for an inspection. The current version of the manual is subject to changes as the EDPS's practices and experiences are evolving. The manual will be formally adopted in the course of 2009 and will be revised and where necessary updated annually.

The current version of the inspection policy guidelines is sent to institutions and bodies before the inspection takes place. The guidelines, after their fine-tuning, will be published on the EDPS's website. They describe, among others things, the main steps in an inspection procedure, the legal basis for inspections, the powers of the EDPS and the role of DPOs during an inspection.

#### **Inspections related to Spring 2007**

In May 2008, the EDPS selected for inspection three institutions and one agency, mainly on the basis of the findings made in the framework of the Spring 2007 exercise. Two inspections were performed in November and December 2008 and two more are planned for the beginning of 2009.

#### *European Economic and Social Committee*

In November 2008, the EDPS inspected the European Economic and Social Committee (EESC)



(Case 2008-574). The inspection was carried out to verify reality regarding the measures taken by the Committee to comply with the regulation in two main fields:

- the status of the DPO inventory and the obligation of controllers to notify the DPO about personal data processing operations (Article 25 of the regulation);
- the processing operations on management of applications for paid traineeship (Case 2005-297) and personal data processing by the medical service (Case 2007-0004). Both processing operations had previously been prior-checked by the EDPS, who made recommendations to improve the level of protection of personal data by the controllers.

*Inventory and notifications:* the controllers who have not yet submitted to the DPO the final notification on data processing to date were interviewed by the EDPS's inspectors as regards the reasons explaining the situation, the measures put in place to ensure further progress in this field and the timelines foreseen to notify the DPO.

*Management of applications for paid traineeship:* the EDPS's inspectors verified and observed a number of items both in the electronic application and in the paper files, *inter alia*, the documents (information) collected from the applicants at the different stages of the application process, information processed in the electronic application, the data retention practices, the security measures related to paper files, the requested information on the role of traineeship advisor and on his/her access to information and requested information on the privacy statement.

*Data processing by the EESC medical service:* the inspectors, *inter alia*, examined the practices at the EESC medical service following the separation of EESC and CoR medical services, verified the security measures related to paper files, requested information on the professional secrecy obligation of staff other than doctors, checked the possible health-related information that the EESC doctor can receive in the case where a staff member decides to go to a doctor of his or her own choice, asked about practices related to the submission of

*note d'honoraires* and to the right of access to the data subjects' own data, as well as to the means of informing data subjects.

The EDPS provided detailed feedback after the inspection, requesting that further progress be made in some of the inspected fields.

#### *European Food Safety Authority*

In December 2008, the EDPS's inspectors carried out an inspection at the premises of the European Food Safety Authority (2008-575). The purpose of the inspection was to verify the measures taken by the EFSA to comply with the regulation in the following main fields:

- the obligation of the controllers to notify the Data Protection Officer (DPO) about personal data processing operations (Article 25 of the regulation);
- checking an inventoried but not yet notified personal data processing operation on staff training policy;
- checking the implementation of EDPS's recommendations made in the prior-checking opinion on the 'Career development and appraisal cycle' (2007-585) (Article 27 of the regulation).

In relation to the Spring 2007 exercise, the EDPS also inquired about the increase of the percentage of DPO working time and of his administrative or secretarial support.

The inspection conclusions will be communicated to EFSA at the beginning of 2009.

#### **Conclusions**

During these inspections, the EDPS has focused on various aspects, such as checking the status of the DPO inventory and notifications to the DPO (which was one item required during the Spring 2007 exercise) and the specific processing operation extracted from the DPO inventory or register, as well as verifying concrete follow-up of the recommendations made in EDPS's prior-checking opinions.

The first inspection experiences show that inspections are a useful means not only to check reality

in Community institutions and bodies, but also to serve as an awareness-raising tool. The EDPS has taken the occasion of these inspections to meet various controllers to explain their obligations under the regulation (EC) No 45/2001 to them. The interviews with various stakeholders and the evaluation of the progress made clearly signalled to the EDPS the level of cooperation between controllers and the DPO. In this respect, inspections can additionally be seen as a means of supporting the work of the DPO.

## 2.6. Administrative measures

Article 28(1) of Regulation (EC) No 45/2001 provides for the right of the EDPS to be informed about administrative measures which relate to the processing of personal data. The EDPS may issue his opinion either following a request from the institution or body concerned or on his own initiative. The term ‘administrative measure’ has to be understood as a decision of the administration of general application relating to the processing of personal data done by the institution or body concerned. This could be the case of implementing measures of the regulation, or internal rules or policies of general application adopted by the administration relating to the processing of personal data.

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

Within the framework of consultations on administrative measures<sup>(19)</sup> envisaged by the Community institutions and bodies, a variety of challenging issues were raised, including for example:

- a new model of medical certificate,
- access to documents containing personal data,

<sup>(19)</sup> Even if there is some overlapping and difference among consultations made in the light of Articles 28(1) and (46)(d), they are both called ‘consultations on administrative measures’ in the context of this report.

- applicable law to certain processing activities,
- transfer to a national tribunal of a medical file,
- retention of data-related disciplinary penalties,
- implementing rules of Regulation (EC) No 45/2001 adopted by the Court of Justice,
- complaints handled by the European Ombudsman.

### 2.6.1. New model of the medical certificate

The Interinstitutional Medical Board (IMB) submitted a draft of a new model of certificate establishing unfitness for work due to illness or accident to the EDPS. The purpose of the new model certificate is to simplify and modernise the Commission’s medical service as well as to offer advantages to the staff (i.e. it will be made available on the intranet and used as needed when consulting a doctor).

The EDPS recommended, inter alia, that the content of the medical data in the draft certificate be reconsidered in the light of the principles of adequacy and relevance. Moreover, the EDPS recommended that an information note be drawn up giving specific information on processing and exhaustive information on the rights of access and rectification and on data storage, according to Articles 11 and 12 of the regulation. This information should also be given on the back of the medical certificate so that both patients and doctors are aware of their rights (Case 2008-312).

### 2.6.2. Access to documents

The Data Protection Officer (DPO) of the European Commission submitted a consultation to the EDPS related to a request for access to documents containing personal data, which seemed to be relevant in the context of a pending case before a national court.

At first, the Commission refused to provide the requesting party with the employment status of a certain person in the Commission, namely whether he or she was a full-time employee in the relevant DG and was working at the Commission on specific given periods.

The Commission invoked Article 8 of Regulation (EC) No 45/2001 and claimed that:

- the requesting party failed to justify the necessity of the transfer of such data;
- a risk of prejudice existed toward the data subject based on the fact that he or she refused to give consent for the disclosure and implication in the litigation.

Nevertheless, the person who requested access to the documents submitted a complaint to the European Ombudsman. The Ombudsman adopted a proposal for a friendly solution to the case suggesting ‘that the Commission could reconsider its contested refusal and provide the complainant with the documentation/information [...] requested unsuccessfully, unless it invokes valid and adequate grounds for not doing so’.

Since the requested information contained personal data, it was evaluated whether the exception foreseen in Article 4(1)(b) of Regulation (EC) No 1049/2001 was applicable. The EDPS followed the methodology described in his background paper on ‘Public access to documents and data protection’<sup>(20)</sup> in order to assess whether the privacy of the individual would be affected in this case. The EDPS considered that he had not been provided with — and did not see — any appropriate reason why the privacy and integrity of the data subject would be at stake and, in any case, why the interest to have his or her data protected in the present case would not be overridden by the interest of public access to documents. As a consequence, the EDPS was of the view that there was no reason to deny such access in the light of Article 4(1)(b) of Regulation (EC) No 1049/2001 (Case 2008-427).

### **2.6.3. Special categories of data: applicable law**

The DPO of the European Union Agency for Fundamental Rights (FRA) consulted the EDPS on a processing operation involving a pool of interested people in EU Member States who wanted to participate in surveys related to fundamental

rights, such as discrimination and criminal victimisation as experienced by selected immigrants and other minority groups. A contract was concluded between the FRA and an external contractor. One of the purposes of the contract was to collect special categories of data, mainly data revealing racial or ethnic origin. The question raised was whether any exemption to Article 10(1) of Regulation (EC) No 45/2001 could be applied in order to overcome the need to receive permission from Member States authorities to conduct the processing activity.

The EDPS explained that since the applicable law to the processing activity under analysis is Regulation (EC) No 45/2001 (the FRA is a European body and the operation falls within Article 3(2) of the regulation), there is no need to request permission from Member States authorities. Nevertheless, the applicable law to the obligations with regard to confidentiality and security is the Belgian law (place of establishment of the processor, where the latter is subject to the national law transposing Directive 95/46/EC). These obligations should therefore be indicated in the contract. As to the sensitivity of the data, the EDPS recommended that special attention be paid to the nature of the consent, as defined in Article 2(h) of the regulation. Moreover, it was recommended to elaborate a privacy statement that strictly complies with Article 11 of the regulation. As it was pointed out, this was also relevant to comply with the obligation to gather an ‘informed’ consent (Case 2008-331).

### **2.6.4. Request from a court for a copy of the full medical file of an official**

The EDPS was consulted by the DPO of an agency in the context of a request from a court asking the agency’s medical service for a copy of the full medical file of an official for the purpose of divorce litigation.

The EDPS considered that in the case under analysis, the controller was subject to the obligation to cooperate with national jurisdictions and, therefore, the processing activity would be justified under this perspective (in the light of Article 5(b) of the regulation which stipulates that

<sup>(20)</sup> July 2005, available at [www.edps.europa.eu](http://www.edps.europa.eu). See in particular Section 4.3.

personal data may be processed only if ‘processing is necessary for compliance with a legal obligation to which the controller is subject’). Nevertheless, the medical service is subject to the obligations derived from the medical secrecy regulations. As a consequence, the cooperation with national jurisdictions has to take place in accordance with the requisites and mechanisms imposed by the national regulations on medical secrecy in the cases of information requested by courts in the frame of legal proceedings.

The EDPS pointed out that, given the sensitivity of the category of data concerned; consent of the data subject would be recommended as a complementary basis for lawfulness (Article 5(d) of the regulation). However, a refusal of the data subject to provide his/her consent would not invalidate the basis under Article 5(b), as explained above. In any case, a refusal to give consent has to be taken into account from the perspective of proportionality and data quality in general.

The EDPS further underlined that, before transferring the medical file, the controller had to ensure that only adequate, relevant and not excessive data are transferred. Considering that the request from the court did not specify the purpose of the processing asked, it was legitimate, in the light of Article 4(1)(b), to require further specification in this regard (Case 2008-145).



Before transferring the medical file to a tribunal, the data controller has to ensure that the data quality principle is respected.

### 2.6.5. Retention of data-related disciplinary penalties

The EDPS expressed his position to the President of the College of Heads of Administration regarding the time limits for keeping the records of penalties in the disciplinary files after they have been executed. It was pointed out that there was a lack of compatibility between the current interpretation of the Staff Regulations and fundamental rights, such as data protection.

In particular, the EDPS underlined that, first of all, Article 27 of Annex IX of the Staff Regulations is in contrast with Regulation (EC) No. 45/2001 due to the fact that the statutory provision indicates the discretionary character of the decision of deletion to be taken by the appointing authority. However, the regulation requires, *inter alia*, that data are kept ‘no longer than is necessary for the purposes for which the data were collected or for which they are further processed’. Consequently, in this context, the EDPS recommended that, in a future revision of the Staff Regulations, it would be advisable to reconsider the present time limits on this basis and to make it mandatory to delete all references to disciplinary measures after the set time limits.

Secondly, the EDPS recommended that a correct interpretation of Articles 10(h) and 10(i) should not imply any contradiction with the true purpose of Article 27. Therefore, the former has to be read ‘without prejudice’ to the latter, and not *vice versa*, so that any harm to the fundamental rights of staff members will be avoided.

Thirdly, disciplinary files should not be kept indefinitely, even after the reference to the sanction has been deleted from the personal file. This does not only infringe Article 4(1)(e) of the regulation but also the principle of not keeping

parallel files in the light of the case law of the Court of First Instance.

Fourthly, the EDPS pointed out that Article 13 of Annex IX uses the term ‘personal file’, meaning ‘disciplinary file of the individual’. Any other interpretation would add nothing to Article 26 of the Staff Regulations and would void Article 13 of any meaning as, for instance, the right of the staff member pursuant to Article 41(2) (b) of the EU Charter of Fundamental Rights (Case 2006-075).

#### **2.6.6. Implementing rules of Regulation (EC) No 45/2001**

The Data Protection Officer (DPO) of the Court of Justice of the European Communities submitted a consultation to the EDPS on a draft decision of the Administrative Committee of the Court of Justice on the implementing rules of Regulation (EC) No 45/2001. The draft only addressed aspects related to Article 24(8) and the annex of the regulation (tasks and obligations of the DPO and controllers) and not those related to the data subjects, as other implementing rules provide for. Within this limited scope, some missing provisions were pointed out, such as the length of the DPO’s mandate and his/her evaluation. Some enlargement of the scope of the DPO’s enquiries was also advised. Nevertheless, the EDPS welcomed the draft as it introduced certain good practices that the EDPS encourages, such as the relationship between the DPO and the court’s information technology services (Case 2008-0658).

#### **2.6.7. Complaints handled by the European Ombudsman**

The EDPS advised the European Ombudsman on the data protection implications of forwarding to the Community institutions involved the Ombudsman’s decisions not to open an inquiry into a certain complaint and the reasons underlying these decisions (Case 2008-608). In this specific case and given the fact that the default rule in the Ombudsman’s office is a public treatment of complaints, the EDPS recommended to inform

the complainant that, unless he or she has already opted for confidentiality, if his or her complaint is declared inadmissible, he or she can again opt for confidentiality after receiving the decision.

## **2.7. Video-surveillance**

### **2.7.1. Guidelines**

During 2008, 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. The first internal working draft of the guidelines was prepared by the end of the year. The draft will be made public for consultation by mid-2009.

The guidelines aim at providing practical advice rather than legal theory. They are intended to be flexible but also to give certainty as to what uses of video-data the EDPS is likely to find objectionable; what steps the institutions need to take before they install a video-surveillance system or update an existing one; and what measures they need to take on an ongoing basis to ensure that data protection concerns continue to be adequately addressed during the operation of a video-surveillance system.

The guidelines recommend the institutions to:

- clearly establish the purpose they wish to achieve with the system;
- carefully analyse whether video-surveillance technology is an efficient and proportionate means to achieve this purpose;
- look for alternative solutions before deciding to use cameras; and
- work together with the DPO of the institution to decide where to site cameras, how to use them, and what safeguards and limitations to introduce to help protect the privacy of the individuals captured on the cameras.

Institutions are also required to keep the video-footage no longer than necessary; strictly limit the range of recipients of the footage; document any use and transfer of the video-footage; and take appropriate security measures to minimise the risk of



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

unauthorised access. In addition, the institutions are also required to provide notice in an appropriate form to the public. The EDPS encourages a multi-layer approach for notice provision, which should include, in addition to on-the-spot notice boards, more detailed information on the website of the institution. Each institution is also required to set up a mechanism to accommodate access requests from members of the public who wish to know what video-data are being processed about them.

The guidelines provide detailed guidance to smaller institutions, among them many agencies, with relatively simple and standard video-surveillance systems.

### 2.7.2. Prior checking

During 2008, the EDPS received two further *ex post* prior-checking notifications on video-surveillance, from JRC IE Petten and from JRC-ITU in Karlsruhe. Just as the four *ex post* prior-checking notifications received in 2007, these were suspended pending the adoption of the EDPS's video-surveillance guidelines.

However, OLAF's closed-circuit television (CCTV) practices, being subject to a proper prior checking procedure, were reviewed by the EDPS (Case 2007-634). This prior-checking opinion is the first among the EDPS's opinions involving video-surveillance. The case concerned

the CCTV system operated by OLAF within its premises in Brussels for security purposes.

On the whole, the EDPS was satisfied with the proportionality of the CCTV system and the data protection safeguards implemented by OLAF. The purposes of the system are clearly delineated, relatively limited and legitimate. Moreover, the location, field of coverage and resolution, and other aspects of the set-up of the CCTV system appear to be adequate, relevant and not excessive in

relation to achieving the specified purposes, also taking into consideration the sensitivity of the information held by OLAF.

Nevertheless, the EDPS made important recommendations to OLAF to reconsider the planned conservation period to ensure that data are kept no longer than necessary for the purposes initially contemplated. The EDPS also recommended that OLAF adopts an internal document describing its CCTV system and providing for appropriate data-protection safeguards. Finally, the EDPS further encouraged OLAF to provide more specific and accurate information to data subjects.

### 2.7.3. Complaint

In 2008, the EDPS continued the follow-up of a citizen's complaint against the CCTV practices of the European Parliament regarding monitoring that takes place outside the Parliament's buildings (Case 2006-0185).

Progress was made in certain important aspects of data-protection compliance. The Parliament reviewed the locations of its cameras and, where it found that private areas of adjacent buildings were in their field of vision, took technical measures to avoid or minimise such occurrence. The Parliament also agreed to provide more comprehensive notice to data subjects regarding its CCTV practices, including

notice on its website. The Parliament now also keeps a registry of all transfers of CCTV footage from the security unit to other *ad hoc* recipients both within and outside the institutions (e.g. all transfers to the police are now recorded in the registry).

With that said, the EDPS did not consider the measures taken by the Parliament fully satisfactory. For example, he would have wished the period of retention of footage outside the premises of the Parliament to be much shorter than they currently are. However, he nevertheless closed the case, at the same time warning the Parliament that once the video-surveillance guidelines will be adopted, they should make steps to align their practices to the EDPS's recommendations. The EDPS also noted the possibility of further follow-up ensuring compliance in a formal *ex post* prior checking procedure or via inspections.

#### 2.7.4. Other requests

When requested, the EDPS also provided informal guidance on video-surveillance practices to DPOs. Recurrent questions related to the manner in which notice should be provided to data subjects and the locations where it would be appropriate and proportionate to install cameras.

In one case, an agency enquired about the proportionality of the use of a hidden camera to detect who the perpetrator of repeated thefts of catering supplies from an individual office is. The EDPS considered the use of hidden cameras disproportionate and recommended the agency to use other methods to detect or deter this behaviour.

At the end of 2008, an enquiry was also made to the EDPS regarding the proportionality of using CCTV cameras in the waiting room of a medical facility. The EDPS is currently reviewing the case.

## 2.8. 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 and has received most attention in 2008 (see Section 4.3).

Other activities of the EDPS with regard to Eurodac involved the interface with consultation on related subjects, such as border policy issues (see Sections 3.4 and 3.6) and preparatory work for the revision of both the Dublin regulation and the Eurodac regulation, on which EDPS opinions were issued in February 2009.

<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).

## 3. Consultation

### 3.1. Introduction

The year 2008 is already the fourth year in which the European Data Protection Supervisor (EDPS) fully exercised his consultative powers as advisor to the Community institutions on proposals for legislation (and related documents). It was again an important year in which the EDPS faced an increase in his activities. He further developed and improved his performance and submitted opinions on an increasing number of substantial proposals for legislation. In 2008, he widened the scope of his interventions to other policy areas of the European Union (EU). Moreover his involvement extended to all stages of the legislative procedure, from the beginning, by reacting to a Green Paper on debtor's assets until the very end, by actively following and sometimes participating in discussions in European Parliament and Council in important files like the European PNR-system and the e-privacy directive.

The objective of the participation of the EDPS 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 opinion of the EDPS is formally issued and then forms part of the legislative process. Several opinions have been presented in the European Parliament's Committee on Civil Liberties, Justice and Home Affairs ('LIBE Committee'), as well as in relevant working groups in the Council.

As in the years before, the EDPS used an inventory of his intentions for the upcoming year. The

'Inventory 2008' was published on the EDPS's website in December 2007. It includes a short analysis of the most important developments as well as the priorities for 2008.

The number of EDPS opinions has increased steadily since the institution started functioning. 14 opinions were issued in 2008. These opinions also reflect the relevant subjects on the policy agenda of the European Commission, the European Parliament and the Council. The majority of the opinions concerned issues related to the area of freedom, security and justice, including the so-called EU 'third pillar' (police and judicial cooperation), as well as border management (within the 'first pillar'). Proposals in this area may promote, for instance, exchange of information between authorities to fight against terrorism and other crimes, possibly involving large-scale databases concerning millions of people. An important development in this area was the adoption in November 2008 of the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters <sup>(22)</sup>.

A number of opinions were also related to cross-border exchange of information, but outside the framework of the fight against terrorism, such as the proposal for a directive on the application of patients' rights in the field of healthcare in December 2008. In general, the EDPS considered that these proposals provided for sufficient justifi-

---

<sup>(22)</sup> Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).





Consultation team discussing a legislative opinion.

cation for the establishment of the considered systems. Nevertheless, he issued recommendations to improve the proposals as to the main elements affecting data protection.

The EDPS does not only make use of opinions to advise the EU institutions in their legislative work. He also uses other instruments of intervention, such as comments. A case in point is the EDPS's preliminary comments on the Commission's EU border management package.

This chapter will look back on the activities of the EDPS in his advisory role in 2008. Individual opinions published in 2008 are summarised in Section 3.3.2. This chapter also describes the consequences for the EDPS of new technological developments, as well as of new developments in the field of policy and legislation.

## 3.2. Policy framework and priorities

### 3.2.1. Implementation of consultation policy

The policy paper entitled 'The EDPS as an advisor to the Community institutions on proposals for legislation and related documents' <sup>(23)</sup> lays down the main elements of how the EDPS envisages fulfilling his tasks in the area of consultation. This paper makes clear how the EDPS proceeds in order to fulfil his assignment in an effective way, as far as the consultation on proposals for legislation is concerned.

<sup>(23)</sup> Available on the EDPS's website ([http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/05-03-18\\_PP\\_EDPSadvisor\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/05-03-18_PP_EDPSadvisor_EN.pdf)).

With this policy paper, the EDPS aims to position himself as a reliable and predictable player in the EU legislative process, in so far as matters concerning the processing of personal data are concerned. This policy paper, adopted in March 2005, has proved to be a solid basis for the activities of the EDPS.

The policy put forward in this paper includes the three following elements.

- The issues on which consultation of the EDPS is required: the scope is wide, since proposals on many subjects can affect the protection of personal data.
- The substance of the interventions by the EDPS: these interventions are based on the general notion that contributions to the legislative process should not only be critical but also constructive.
- The role the EDPS envisages playing within the EU institutional framework: the advisory task of the EDPS has become more and more self-evident for the institutions.

The policy paper foresees different moments of intervention. The European Commission's services normally involve the EDPS before the formal adoption of a Commission proposal, quite often in parallel with its internal inter-services consultation. At this stage, the EDPS provides informal comments. After the adoption of his opinion, the EDPS also maintains informal contacts with the Council, through its Presidency and its Secretariat General. On several occasions, the EDPS clarified and discussed his opinions within the Council's working groups dealing with the considered legislative proposal. The same activities were undertaken in relation to the LIBE Committee and other Parliament committees dealing with the initiative. In addition, the EDPS has initiated informal contacts with the European Parliament — both members and secretariats — while also remaining available for more general discussions, such as in public hearings. A new development in 2008 was the close involvement in legislative dossiers in later stages of the

legislative procedure, in particular with regard to the European PNR system and the e-privacy directive.

Special attention will be given in 2009 to how to advise the Commission in cases where it does not adopt a proposal (to the Council and/or the European Parliament), but decides itself. This situation applies in the following cases:

- implementing legislation by the Commission (with ‘comitology’ or not);
- Commission decisions declaring the adequate level of data protection in a third country pursuant to Article 25(6) of Directive 95/46/EC;
- publication of a Commission communication.

In those specific cases, a formal opinion following the adoption by the Commission cannot influence the text of the instrument.

On 28 April 2008, the EDPS presented another policy paper entitled ‘The EDPS and EU research and technological development’. The EDPS has decided to closely follow the seventh framework programme (FP7) for research and technological development (RTD), launched by the Commission at the end of 2006. He decided to develop several possible models of contribution to targeted research projects of the ongoing FP7. The aim of these contribution models is to advise the Commission and/or project developers in their efforts to use privacy and data-protection-friendly RTD methodologies and encourage the development of technologies and processes that will promote and reinforce the effectiveness of the EU data protection legal framework. The policy paper sets out the main elements of the EDPS’s policy in this area (see Section 3.6.5).

### 3.2.2. Inventory 2008

Each year, the EDPS publishes an inventory of his intentions in the coming year. The Inventory 2008 was published in December 2007 on the EDPS’s website

This inventory forms part of the annual work cycle of the EDPS. Once a year, the EDPS reports

retrospectively on his activities in the annual report. In addition, the EDPS publishes an inventory in the area of consultation for the following year. As a result, the EDPS reports twice a year on his activities in this area. An important part of his working method is the selection and planning needed in order to be effective as an advisor.

The main sources of the inventory are the Commission’s legislative and work programme and several related planning documents of the Commission. In the preparation process, several stakeholders within the Commission have been given the possibility to provide their input.

The inventory 2008 consists of the following elements:

- an introductory part which includes a short analysis of the context, as well as the priorities of the EDPS for 2008;
- an annex to the relevant Commission proposals and other documents that have been recently adopted or are programmed, and that require the attention of the EDPS.

The annex relating to 2008 and published in December 2007 has been updated twice in the course of 2008 (in May and in October).

### Results

The annex to the Inventory 2008 listed 34 important documents (highlighted as ‘red’) on which the EDPS intended to issue an opinion or take a similar action. This purpose has led to the following results.

Opinions issued	13 documents (incl. 3 by end-December 2007)
Comments / other EDPS acts	4 documents
Reaction through the Article 29 Working Party	1 document
Commission proposals and/or EDPS opinions postponed to 2009	14 documents <sup>(1)</sup>
No further EDPS action	2 documents

<sup>(1)</sup> Seven out of these 14 are in the area of Eurodac and SIS. They are reclustered in Inventory 2009.

Furthermore, the list contained 33 other topics with a lower priority on which the EDPS might have issued an opinion or reacted in another way. The state of play at the end of 2008 shows a diverse picture.

EDPS's continuous attention (research programmes, general issues/subjects such as public health or large-scale information systems)	17 documents
EDPS's involvement in 2008 (comments or other actions)	3 documents
Deleted from list without further action by the EDPS	7 documents
Commission activity postponed to 2009	4 documents
Upgraded to 'red' issue (opinion issued in 2008)	2 documents

### Priorities for 2008

**Priority 1:** The effects of the Lisbon Treaty, although its entry into force now *inter alia* depends on a second referendum in Ireland, has been closely followed and commented upon by the EDPS in 2008. The Treaty will have a great impact on data protection.

**Priority 2:** The EDPS has continued to focus on the storage and exchange of information in the area of freedom, security and justice with emphasis amongst other things on ensuring an adequate legal framework for data protection in this area, taking into account the limited scope of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

**Priority 3:** The developments taking place in the information society have again been closely followed and commented on, such as RFID and ambient intelligence, as a follow up to the European Commission's communication on RFID and the related EDPS's opinion. In this context, much emphasis was placed on the revision of the e-privacy directive.

**Priority 4:** The EDPS's opinion on the future of Directive 95/46/EC has been followed up. The EDPS participated in activities relating to the full implementation of the directive. He is closely involved in the various debates on the future of the directive.

**Priority 5:** A few specific areas of EU action have been brought into focus, such as public health, the relation between data protection and the collection and use of statistics, and further activities relating to public access to documents.

**Priority 6:** Many activities centred on the transfer of data to third countries, in particular the transfer of passenger data and the developments regarding possible transatlantic principles (mainly common to EU and USA) on exchange of information for law enforcement purposes.

### 3.2.3. Inventory 2009

#### Priorities for the EDPS for 2009

The policy of the EDPS will not shift from the directions indicated in the Inventory 2008. It can be noted that in 2008, the impact assessments mentioned in the Commission legislative and work programme 2008 have given appropriate attention to privacy and data protection.

The priorities for 2009 will build on the priorities over 2008, taking into account the developments that have taken place since then. Aside from new proposals, special attention will be paid to the Commission's communication on the Stockholm programme in the area of freedom, security and justice<sup>(24)</sup>. The main aim of this initiative is to define the priorities and objectives for the future development of the EU in this area, and to determine the means and initiatives to best achieve them. This initiative would include a global pact on migration, e-justice and an action plan on drugs. It gives the EDPS the opportunity to reflect on his priorities for

<sup>(24)</sup> Commission's communication on the Stockholm programme in the area of freedom, security and justice, 2008/JLS/119.

the five coming years. He shall react in the preparation stage and will adopt an opinion after adoption. This also has the advantage of coinciding with the new EDPS's mandate that will start in 2009.

### 3.3. Legislative opinions

#### 3.3.1. General remarks

The EDPS adopted 14 legislative opinions in 2008. As in previous years, a substantial part of the opinions relate to the area of freedom, security and justice, both in the first and third pillars. This area represents almost half of the legislative opinions issued, namely six out of 14. The proposal to modify Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents also had special attention of the EDPS. Other important initiatives on which the EDPS adopted opinions covered the following issues: the internal market information system (IMI), computerised reservation systems (CRS), road safety, European statistics and cross-border healthcare.

From the overview of the 14 opinions, one may conclude that, in most cases, the EDPS supported the proposals but requested specific additional data-protection safeguards.

#### Exchange of information

The exchange of information, in particular the establishment of information systems and access by different authorities to those systems for specific purposes was a key focus area for the EDPS. Cross-border exchange of information is becoming more widely used nowadays.

In 2008, the EDPS adopted opinions on information exchange that were proposed in the framework of the internal market information System (IMI), Eurojust, road safety, the protection of children using the Internet, ECRIS, the EU-US high-level contact group on information sharing, and the European e-justice strategy. The EDPS analysed the legal consequences linked to the development of different large-scale information and technology systems. The conclusion is that the need for such exchange of information must be properly and carefully assessed in each case. Moreover, when such

exchange of information is established, specific data-protection safeguards need to be implemented.

Because of the risks of illegitimate use, legal obligations that lead to substantial databases create particular risks for the data subjects. The EDPS was repeatedly concerned about the lack of safeguards surrounding the exchange of personal data with third countries. Several proposals included provisions for such exchanges and the EDPS pointed out that mechanisms ensuring common standards and coordinated decisions on adequacy should be put in place. Exchanges with third countries should only be allowed if they ensure an adequate level of protection of personal data, or if the transfers fall within the scope of one of the derogations laid down by Directive 95/46/EC.

#### New technologies

On several occasions, the EDPS addressed the issue of the use of new technologies. He repeatedly called for ensuring that data protection issues are taken into account at the earliest possible stage ('privacy-by-design'). He also highlighted that technology tools should be used not only to ensure the exchange of information, but also to enhance the rights of the persons concerned. In the ECRIS and e-justice cases, the EDPS welcomed the possibility for the person concerned to request information on his/her own records to the central authority of a Member State, provided that the person is or has been a resident or a national of the requested or requesting Member State. The idea of using as a 'one-stop-shop' the authority which is closer to the person concerned was also put forward by the EDPS in the area of coordination of social security systems. Therefore, the EDPS encourages the Commission to foster technology tools and, in particular, online access, allowing citizens to be in better control of their personal data even when they move between different Member States.

#### Quality of data

The quality of data was an important theme. A high level of accuracy of data is needed to avoid ambiguity concerning the content of information processed. It is therefore imperative that the accuracy be regularly and properly checked. Moreover, a high level of data quality represents not only a basic guarantee for the data subject, but also facilitates the efficient use for those who process the data.

### 3.3.2. Individual opinions

#### Internal market information system (IMI)

On 22 February 2008, the EDPS presented an opinion on the Commission decision concerning the implementation of the internal market information system (IMI) <sup>(25)</sup>. The internal market information system (IMI) is an information technology tool that allows competent authorities in Member States to exchange information with each other in the implementation of the internal market legislation. IMI is funded under the IDABC programme ('Interoperable delivery of European e-government services to public administrations, businesses and citizens').

The main recommendation of the EDPS referred to the need for a solid legal basis for the IMI decision. The EDPS was of the opinion that the current legal basis (a decision under the IDABC programme) does not provide for the necessary legal certainty since there are doubts about the binding nature of this instrument. The EDPS furthermore provided for a number of suggestions on the provisions regulating the data protection aspects of IMI. These relate to transparency and proportionality; joint control and allocation of responsibilities; notice to data subjects; rights of access, objection, and rectification; data retention; security measures and joint supervision.

#### Security features and biometrics in passports

On 26 March 2008, the EDPS presented an opinion on the proposal for a regulation of the European Parliament and of the Council amending the Council regulation on standards for security features and biometrics in passports and travel documents issued by Member States, although he had not been consulted on this proposal <sup>(26)</sup>.

Together with security elements, biometric data aim at strengthening the link between the passport and

the holder of this document. In view of harmonising exceptions to the biometrics passport, the proposal has added the following measures: children under the age of six years are exempted from the obligation to give fingerprints, and persons who are physically unable to give fingerprints should also be exempted from this requirement. Additionally, the proposal introduces the obligation of 'one person — one passport', which is described as a supplementary security measure and additional protection for children.

The EDPS advised that the proposed regulation be amended to:

- define the age limit for children by a consistent and in-depth study which is to identify properly the accuracy of the systems obtained under real conditions, and to reflect the diversity of the data processed; this study should be executed by a European institution with clear expertise and adequate facilities in this field;
- introduce an age limit for elderly, which can be based on similar experiences (US Visit: age 79), as an additional exemption; such exemptions should in no case stigmatise or discriminate the individuals concerned;
- the principle of 'one person—one passport' should be applied only to children above the relevant age limit;
- 'breeder' documents: additional measures should be proposed to harmonise the production and the use of documents required in Member States to issue passports ('breeder' documents);



Biometrics in passports: an authentication scheme requesting stringent safeguards.

<sup>(25)</sup> Opinion of 22 February 2008 on the Commission decision of 12 December 2007 concerning the implementation of the internal market information system (IMI) as regards the protection of personal data (2008/49/EC) (OJ C 270, 25.10.2008, p. 1).

<sup>(26)</sup> Opinion of 26 March 2008 on the proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OCJ 200, 6.8.2008, p. 1).

- better harmonise the implementation of Regulation (EC) No 2252/2004: only decentralised storage of biometric data collected for Member States' passports and common error rates for the enrolment and matching process should be implemented.

### E-privacy

On 10 April 2008, the EDPS advised on the proposal for a directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications, also referred to as the 'e-privacy directive')<sup>(27)</sup>.

The proposal aims at enhancing the protection of individuals' privacy and personal data in the electronic communications sector. This is done not by entirely reshaping the existing e-privacy directive but rather by proposing *ad hoc* amendments to it, which mainly aim at strengthening the security-related provisions and improving the enforcement mechanisms.

This opinion addressed the following topics:

- the scope of the e-privacy directive, in particular, the services concerned (proposed amendment to Article 3(1));
- the notification of security breaches (proposed amendment creating Articles 4(3) and 4(4));
- the provisions on cookies, spyware and similar devices (proposed amendment to Article 5(3));
- the legal actions initiated by electronic communication services providers and other legal persons (proposed amendment creating Article 13(6); and
- the strengthening of the enforcement provisions (proposed amendment creating Article 15(a).

The opinion has been followed up by an intensive involvement of the EDPS in the further legislative procedure (see Section 3.6).

<sup>(27)</sup> Opinion of 10 April 2008 on the proposal for a directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications) (OJ C 181, 18.7.2008, p. 1).

### Computerised reservation systems

On 11 April 2008, the EDPS presented an opinion on the proposal for a regulation of the European Parliament and of the Council on a code of conduct for computerised reservation systems<sup>(28)</sup>.

The objective of the proposal is to update the provisions of the code of conduct for computerized reservation systems that was established in 1989 by Council Regulation (EEC) No 2299/89. The code appears to be increasingly ill-adapted to the new market conditions, and would need simplification in order to reinforce competition — while maintaining basic safeguards, and ensuring the provision of neutral information to consumers.

The EDPS's conclusions were as follows.

- He welcomed the inclusion in the proposal of data protection principles that specify the provisions of Directive 95/46/EC. These provisions enhance legal certainty, and could usefully be complemented by additional safeguards on three points: ensuring the fully informed consent of data subjects for the processing of sensitive data; providing for security measures taking into account the different services offered by CRSs, and the protection of marketing information.
- With regard to the scope of application, the criteria that make the proposal applicable to CRSs established in third countries raised the question of its practical application, in a coherent way with the application of the *lex generalis*, i.e. Directive 95/46/EC.
- To ensure the effective implementation of the proposal, the EDPS considered that there was a need for a clear and comprehensive view on the whole area of CRSs, taking into account the complexity of the CRS network and the conditions of access by third parties to personal data processed by CRSs.

### Eurojust

On 25 April 2008, the EDPS advised on the initiative of a group of Member States with a view to adopting a Council decision concerning

<sup>(28)</sup> Opinion of 11 April 2008 on the proposal for a regulation on a code of conduct for computerised reservation systems (OJ C 233, 11.9.2008, p. 1).

the strengthening of Eurojust and amending Decision 2002/187/JHA <sup>(29)</sup>.

The initiative aims at further enhancing the operational effectiveness of Eurojust.

The EDPS suggested various amendments to the proposal, including the following.

- A reference should be made to the Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. The lists of personal data that may be processed under the Council decision should remain closed lists.
- A provision similar to Article 38(5)(a) of the proposal for a Council decision establishing the European Police Office (Europol) should be included in order to establish that the provisions of Regulation (EC) No 45/2001 shall apply to the processing of personal data relating to Eurojust staff.

### Road safety

On 8 May 2008, the EDPS presented an opinion on the proposal for a directive of the European Parliament and of the Council facilitating cross-border enforcement in the field of road safety <sup>(30)</sup>. The proposal constitutes a measure taken in the global objective of reducing fatalities, injuries and material damage resulting from traffic accidents. In this context, the proposal intends to establish a system to facilitate the cross-border enforcement of sanctions for specified road traffic offences. In order to contribute to a non-discriminatory and more effective enforcement towards traffic offenders, the proposal foresees the establishment of a system of cross-border exchange of information between Member States.

The opinion issued the following recommendations:

- On information of the data subjects: the way data subjects will be informed of the fact they have specific rights will depend on the format of the

offence notification. It is therefore important that the proposal lists all information relevant for the data subject, in a language that he or she understands.

- On security aspects: while the EDPS has no objection to the use of an already existing infrastructure to exchange the information, he insisted that this should not lead to interoperability with other databanks; he welcomed the limit put in the proposal on the possibilities of use of the data by Member States other than the one where the offence was committed.
- The EDPS is available for further consultation with regard to the common rules to be elaborated by the Commission on technical procedures for the electronic exchange of data between the Member States and, in particular, with regard to the security aspects of these rules.

### European statistics

On 20 May 2008, the EDPS issued his opinion on the proposal for a regulation on European statistics <sup>(31)</sup>. The proposal aims to revise the existing basic legal framework governing the production of statistics at European level with a view to adapting it to the current reality and to improving it to meet future developments and challenges.

The EDPS welcomed the proposal, as the initiative would give a firm and general legal basis to the development, production and dissemination of statistics at a European level. However, the EDPS stressed the following points.

- The EDPS expects to be consulted on the sectoral legislation which could be adopted on statistics by the Commission in order to implement this regulation, once it has been adopted.
- The proposed concept of ‘statistical data subject’ should be reconsidered in order to avoid confusion with data-protection concepts.
- The principle of data quality should be taken into consideration in the quality assessment of the Commission.
- The ambiguity of the concept of ‘anonymisation’ of data should be considered in the context of dissemination of data.

<sup>(29)</sup> Opinion of 25 April 2008 on the initiative of 14 Member States with a view to adopting a Council decision concerning the strengthening of Eurojust and amending Decision 2002/187/JHA (OJ C 310, 5.12.2008, p. 1).

<sup>(30)</sup> Opinion of 8 May 2008 on the proposal for a directive of the European Parliament and of the Council facilitating cross-border enforcement in the field of road safety (OJ C 310, 5.12.2008, p. 9).

<sup>(31)</sup> Opinion of 20 May 2008 on the proposal for a regulation of the European Parliament and of the Council on European Statistics (COM(2007) 625 final) (OJ C 308, 3.12.2008, p. 1).



Children are an easy target on the internet.  
Appropriate data protection measures are needed to protect them.

### Protecting children using the Internet

On 23 June 2008, the EDPS adopted an opinion on the proposal for a decision of the European Parliament and of the Council establishing a multi-annual Community programme on protecting children using the Internet and other communication technologies <sup>(32)</sup>.

The EDPS welcomed the fact that the programme intends to focus on the development of new technologies and on the elaboration of concrete actions to enhance the effectiveness of the protection of children. The protection of personal data is an essential prerequisite to the safety of children online. Misuse of children's personal information must be prevented, using the orientations proposed in the programme, and especially the following:

- ensuring awareness of children and other stakeholders like parents and educators;
- promoting the development of best practice by the industry;
- promoting the development of privacy-compliant technological tools;

<sup>(32)</sup> Opinion of 23 June 2008 on the proposal for a decision establishing a multiannual Community programme on protecting children using the Internet and other communication technologies (OJ C 2, 7.1.2009, p. 2).

— favouring the exchange of good practice and practical experience amongst relevant authorities, including data-protection authorities.

These actions should be developed without overlooking the fact that the protection of children takes place within an environment where the rights of others might be at stake. In particular, the EDPS recalled that the surveillance of telecommunication networks should be the task of law enforcement authorities.

The EDPS noted that this programme constitutes a general framework for further concrete actions. He recommended that data protection authorities be closely involved when it comes to the definition of practical projects.

### Public access to documents

On 30 June 2008, the EDPS presented an opinion on the proposal for a regulation regarding public access to European Parliament, Council and Commission documents <sup>(33)</sup>. The proposal was preceded by a public consultation. After the adoption of the proposal in June 2008, a public hearing took place in the Parliament's LIBE Committee. On that occasion, the representatives of the European Commission emphasised that the proposal reflected the current state of thinking, but that they were open to discuss the text and consider input for the improvement of the proposal, not excluding alternatives.

The EDPS saw this open approach as an opportunity and aimed at enriching the discussion with an alternative text for the proposed Article 4(5), a provision dealing with the delicate relation between access to documents and the rights to privacy

<sup>(33)</sup> Opinion of 30 June 2008 on the proposal for a regulation regarding public access to European Parliament, Council and Commission documents (OJ C 2, 7.1.2009, p. 7).



and to the protection of personal data. This provision was meant to give effect to the Judgement of the Court of First Instance in Bavarian Lager (Case T-194/04). The EDPS supported the reasons behind replacing Article 4(1)(b) by a new provision to some extent, but did not support the provision itself.

This provision was criticised for the following reasons:

- The EDPS was not convinced that this was the appropriate moment for change, while an appeal where fundamental issues were at stake was pending before the European Court of Justice.
- The proposal did not provide the appropriate solution as it consists of a general rule (second sentence of Article 4(5) that:
  - does not reflect the judgement of the Court of First Instance in Bavarian Lager;
  - does not do justice to the need for a right balance between the fundamental rights at stake;
  - is not viable since it refers to EC legislation on data protection that does not provide a clear answer when a decision on public access must be made.
- It consists of a specific rule (first sentence of Article 4(5) that is in principle well defined, but with a scope that is far too limited.



EDPS contributes to the right balance between public access to EU documents and privacy.

## ECRIS

On 16 September 2008, the EDPS advised on the proposal for a Council decision on the establishment of the European criminal records information system (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA <sup>(34)</sup>.

The proposal aims to implement Article 11 of the Council framework decision on the organisation and content of the exchange of information extracted from criminal records between Member States in order to build and develop a computerised information-exchange system between Member States. It establishes ECRIS and also sets up the elements of a standardised format for the electronic exchange of information, as well as other general and technical implementation aspects in order to organise and facilitate the exchanges of information.

The EDPS supported the proposal and made some observations.

- The responsibility of the Commission for the common infrastructure of the system, as well as the applicability of Regulation (EC) No 45/2001, should be clarified to better ensure legal certainty.
- The Commission should also be responsible for the interconnection software of ECRIS — and not Member States as provided in the proposal — in order to improve the effectiveness of the exchange and to allow better supervision of the system.
- The use of automatic translations should be clearly defined and circumscribed, so as to favour mutual understanding of criminal offences without affecting the quality of the information transmitted.

## Transparency of debtors' assets

In March 2008, the European Commission issued a Green Paper on transparency of debtors'

<sup>(34)</sup> Opinion of 16 September 2008 on the proposal for a Council decision on the establishment of the European Criminal Record Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA (OJ C 42, 20.2.2009, p. 1).

assets<sup>(35)</sup>. The analysed Green Paper focuses on possible measures at EU level that can be adopted with a view to ‘improve the transparency of the debtor’s assets and the right of creditors to obtain information whilst respecting the principles for the protection of debtor’s privacy’ pursuant to the provisions of Directive 95/46/EC.

On 22 September 2008, the EDPS presented an opinion on the Green Paper<sup>(36)</sup> in which he recommended that possible legislative actions stemming from the Green Paper should ensure that the processing of personal data carried out by the whole range of enforcement authorities is clearly based on at least one of the legal grounds laid down by Article 7 of Directive 95/46/EC. He also asked that the proportionality principle should be duly taken into account and that any measures on transparency of debtors’ assets respect the purpose limitation principle and that any necessary exception complies with the conditions laid down in Article 13 of Directive 95/46/EC.

#### **EU–US high-level contact group on information sharing**

On 11 November 2008, the EDPS presented an opinion on the final report by the EU-US high-level contact group on information sharing and privacy and personal data protection<sup>(37)</sup>. The report tends to identify common principles for privacy and data protection as a first step towards exchange of information with the United States to fight terrorism and serious transnational crime.

The EDPS’s opinion pointed out that the impact of a transatlantic instrument on data protection should be carefully considered in relation to the existing legal framework and the consequences for citizens. He expressed his preference for a legally binding agreement in order to provide sufficient legal certainty.

<sup>(35)</sup> COM(2008) 128 final.

<sup>(36)</sup> Opinion of 22 September 2008 on the Commission Green Paper on the effective enforcement of judgements in the European Union: the transparency of debtors’ assets — COM(2008) 128 final (OJ C 20, 27.1.2009, p. 1).

<sup>(37)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11\\_High\\_Level\\_Contact\\_Group\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf)

In addition, the EDPS called for more clarity and concrete provisions, especially on the following aspects:

- a thorough adequacy finding, based on essential requirements addressing the substance, specificity and oversight aspects of the scheme: the EDPS considered that the adequacy of the general instrument could only be acknowledged if combined with adequate specific agreements on a case-by-case basis;
- a circumscribed scope of application, with a clear and common definition of law enforcement purposes at stake;
- strong oversight and redress mechanisms available to data subjects, including administrative and judicial remedies;
- effective measures guaranteeing the exercise of their rights to all data subjects, irrespective of their nationality;
- involvement of independent data protection authorities, in relation especially to oversight and assistance to data subjects.

The EDPS additionally recommended the development of a roadmap towards a possible agreement at a later stage. He also called for more transparency with regard to the process of elaboration of the data protection principles. Only with the involvement of all stakeholders, including the European Parliament, could the instrument benefit from a democratic debate and gain the necessary support and recognition.

#### **Cross-border healthcare**

On 2 December 2008, the EDPS advised on a proposal of the European Parliament and of the Council on the application of patients’ rights in cross-border healthcare<sup>(38)</sup>. The proposal aims at establishing a Community framework for the provision of cross-border healthcare within the EU, for those occasions where the care patients seek is provided in another Member State than in their home country.

<sup>(38)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-02\\_Cross-border\\_healthcare\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-02_Cross-border_healthcare_EN.pdf)

The EDPS supports the initiatives of improving the conditions for cross-border healthcare. However, he expressed concerns about the fact that EC healthcare-related initiatives are not always well coordinated with regard to ICT use, privacy and security, thus hampering the adoption of a universal data protection approach towards healthcare.

The EDPS welcomed that reference to privacy is made within the proposal. He suggested that:

- a definition of health data should be included, covering any personal data that can have a clear and close link with the description of the health status of a person; this should in principle include medical data, as well as administrative and financial data relating to health;
- a specific article on data protection should clearly set the overall picture, describing the responsibilities of the Member States of affiliation and treatment and identifying the main areas for further development, i.e. security harmonisation and privacy integration, especially in e-health applications;
- the notion of ‘privacy by design’ is incorporated in the proposed Community template for e-prescription.

#### European e-justice strategy

On 19 December 2008, the EDPS issued an opinion on a Commission communication on a European e-justice strategy <sup>(39)</sup>. The communication aims to propose a strategy that intends to increase citizens’ confidence in the European area of justice. E-justice’s primary objective should be to help justice to be administered more effectively throughout Europe, for the benefit of the citizens. The EU’s action should enable citizens to access information without being hindered by the linguistic, cultural and legal barriers stemming from the multiplicity of systems.

<sup>(39)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-19\\_eJustice\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-19_eJustice_EN.pdf).

The EDPS supported the proposal, taking into account the observations made in his opinion, which included:

- taking into account Council Framework Decision 2008/977/JHA on the protection of personal data in the field of police and judicial cooperation in criminal matters;
- including administrative procedures in e-justice;
- maintaining a preference for decentralised architectures with clear responsibilities for all actors processing personal data within the envisaged systems; the Commission should be responsible for common infrastructures;
- ensuring that the interconnection and interoperability of systems duly takes into account the purpose limitation principle;
- ensuring that processing of personal data for purposes other than those for which they were collected should respect the specific conditions laid down by the applicable data-protection legislation.

### 3.4. Comments

Comments are a simpler instrument of intervention than legislative opinions. The instrument is used by the EDPS in cases where a full legal analysis is not deemed useful. The comments contain a policy analysis, and provide constructive recommendations in order for the proposed actions to properly comply with and promote the data protection principles.

#### Border management

On 3 March 2008, the EDPS made preliminary comments on three communications from the European Commission aimed at developing the EU’s external border management <sup>(40)</sup>. The comments focused on those measures raising data protection concerns, in particular the creation of an entry/exit system that would include the recording of travellers’ information, the use of biometric

<sup>(40)</sup> COM(2008) 69, COM(2008)68 and COM(2008)67.

data and, possibly, the creation of a large-scale EU database to store these data.

The EDPS emphasised that, although driven by a legitimate goal — i.e. making EU borders more secure while facilitating travel for bona fide travellers — the proposed measures demand careful scrutiny as they involve large processing operations of personal data, with significant privacy intrusions. The EDPS stressed that it is crucial that the impact on the privacy rights of individuals crossing the EU borders is adequately taken into account. A lack of data protection safeguards would not only mean that the individuals concerned might suffer unduly from the proposed measures, but also that the measures will be less effective, or even counter productive, by diminishing public trust in government action.

The EDPS's comments also included general remarks as regards the piling up of legislative proposals in the area, heavy reliance on biometric data and a lack of evidence supporting the need for new data systems.

#### **Commission IMI decision — Follow up of the EDPS's opinion of 22 February 2008**

On 14 July 2008, the EDPS answered a letter of the Commission proposing a way forward towards a more complete implementation of the necessary data protection safeguards for the internal market information system (IMI).

The EDPS agreed that the adoption of data protection guidelines in the form of a Commission recommendation was a significant and welcome step towards the establishment of a comprehensive data protection framework for IMI. He emphasised that IMI, whose scope is currently limited to information exchanges under the services and professional qualifications directives, would gradually broaden its scope to additional areas of internal market legislation. This would lead to increased complexity and an increasing number of participating authorities and data exchanges. In this context, the EDPS believes that it will be necessary to provide for specific data protection safeguards that go beyond the existing applicable data protection legislation, in legally binding Community legislation.

#### **Universal Service and e-privacy — Follow up of the EDPS's opinion of 10 April 2008**

As to the universal service and e-privacy directives, the EDPS commented on selected issues that arose from the IMCO report on the review of Directive 2002/22/EC. On 2 September 2008, the EDPS expressed his concern about some *ad hoc* amendments contained in the IMCO report which, if adopted, would result in weakening personal data and privacy protections of individuals using the Internet (see also Section 3.6).

### **3.5. Court interventions**

The EDPS has the right to intervene in cases before the Court of Justice of the European Communities that are relevant to his task. This right extends to all Community matters concerning the processing of personal data.

The right to intervene is based on Article 47 of Regulation (EC) No 45/2001 and extends to the Court of First Instance and the Civil Service Tribunal. In his interventions, the EDPS aims at clarifying the perspective of data protection.

On 1 July 2008, the EDPS participated in the hearing in Case C-301/06, *Ireland v Council and Parliament*. The EDPS defended that the data retention directive (2006/24/EC) was rightfully based on Article 95 of the EC Treaty <sup>(41)</sup>.

Furthermore, the EDPS requested intervention in the following cases:

- Case C-518/07 (*Commission v Germany*) before the European Court of Justice on the independence of data protection authorities,
- Case T-3/08 (*Coédo Suárez v Council*) before the Court of First Instance on the right of access in the data protection regulation,
- Case F-35/08 (*Pachtitis v Commission*) before the Civil Service Tribunal on the right of access in the data protection regulation,
- Case F-48/08 (*Ortega Serrano v Commission*) before the Civil Service Tribunal on the right of access in the data protection regulation,

---

<sup>(41)</sup> The pleadings of the EDPS can be found on the EDPS's website.

- Case T-383/08 (*New Europe v. Commission*) before the Court of First Instance on public access to documents.

The courts have admitted the EDPS to intervene in the first three cases. In case F-48/08, the appeal itself was declared not admissible, whereas in case T-382/08 the court has not yet decided on the request of the EDPS.

The EDPS submitted substantive statements in three cases.

- In Case C-518/07 the EDPS submitted a statement in intervention supporting the Commission;
- In Case C-28/08 P (*Commission v Bavarian Lager*), the EDPS issued a response to the appeal of the Commission (Case C-28/08 P) against the judgment of 8 November 2007 of the Court of First Instance in the Bavarian Lager Case T-194/04. He also reacted — as a party in the procedure — to the submissions of the interveners;
- In Case T-374/07 (*Pachtitis v Commission and EPSO*) submitted a statement in intervention supporting the Commission.

### 3.6. Other activities

#### 3.6.1. E-privacy

The Commission's proposal for the revision of the e-privacy directive required permanent attention from the EDPS throughout the year <sup>(42)</sup>.

On 2 September 2008 the EDPS provided comments on selected issues related to the processing of traffic data and the protection of intellectual property rights <sup>(43)</sup>. Later that month the European Parliament adopted a legislative resolution on the e-privacy directive <sup>(44)</sup>. Among the important changes was the inclusion of information society

<sup>(42)</sup> See also section 3.3.2 on individual opinions.

<sup>(43)</sup> See Section 3.4.

<sup>(44)</sup> European Parliament legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)).



The EDPS provided extensive input to the European Commission, Parliament and Council on the review of the e-privacy directive.

service providers under the scope of the obligation to notify security breaches.

The EDPS welcomed this change and also welcomed the amendment enabling legal and natural persons to file actions for infringement of any provision of the e-privacy directive. On 17 September 2008, the EDPS presented his views at a hearing organised by members from different political groups in the European Parliament. On other occasions, he exchanged views with members of the European Parliament and other stakeholders about issues such as security breach notification, the processing of IP addresses and standardisation for the purposes of designing privacy-friendly products.

In November 2008, the Council reached a political agreement on a review of the rules on the telecoms package, including the e-privacy directive. The Council modified essential elements of the proposal and did not accept many of the amendments adopted by the European Parliament. The EDPS showed concern about the content of the common position because safeguards for the citizens are deleted or substantially weakened. As a result, the level of protection afforded to individuals in the common position is substantially weakened.

It is for these reasons that the EDPS announced a second opinion which was finally adopted on 9 January 2009 (to be discussed in the 2009 annual report).

### 3.6.2. PNR

As in earlier years, the EDPS was closely involved in PNR-related matters. In 2008 much energy was put into the follow up of the proposal for a Council framework decision on the use of passenger name records (PNR) for law enforcement purposes<sup>(45)</sup>, the EU internal scheme for the collection and use of airline passenger data entering or leaving the EU. The EDPS was closely involved in the developments under the French Presidency, questioning in particular the necessity and the proportionality of the scheme. The work will continue under the Czech and Swedish Presidencies.

The estimated date of adoption of the proposal by the Council is uncertain. The EDPS intends to continue to follow the development closely and will probably issue a second opinion.

### 3.6.3. Implementation SIS and border policy

As stated above (Section 3.1), the EDPS gives a broad interpretation of his advisory task on proposals for legislation. Nevertheless, the EDPS endeavours to vary the intensity of the accomplishment of the advisory task, according to the impact of proposals on the protection of personal data. At present, the proposals in the area of freedom, security and justice are of great importance. Crucial issues in this area are the sharing of information in the framework of police and justice cooperation, as well as issues related to large-scale information systems like Eurodac, the visa information system (VIS) and the second generation Schengen information system (SIS II). The SIS II consists of a central database called the 'Central Schengen information system' (CS-SIS) for which the Commission ensures the operational management connected to national access points defined by each Member State (NI-SIS). Sirene authorities shall ensure the exchange of all supplementary information (information connected to the SIS II alerts but not stored in the SIS II).

---

<sup>(45)</sup> COM(2007) 654.

On 30 June 2008, the EDPS presented two interventions at a round table organised by the LIBE Committee of the European Parliament, involving both the European Parliament and representatives from national parliaments. The topic of this round table was 'Freedom and security in the integrated management of the European Union's borders — Exchange of views on the new Schengen information system (SIS II), Frontex, Eurosur, entry exit system, profiling'.

The first intervention of the EDPS addressed the issue of 'Data protection implications in the migration from SIS I+ to SIS II'. With regard to the Central Unit, which shall be under the EDPS's supervision, the EDPS underlined that he intends to conduct an audit during the very first stage of operations, i.e. to provide for a benchmarking tool for future use. He also reminded how crucial the cooperation was with national data-protection authorities and the Schengen Joint Supervisory Authority in order to ensure a smooth transition between the two systems.

In a second intervention during a session devoted to 'Protecting freedom, security and privacy in the future EU border management', the comments of the EDPS on the 'border package' were mentioned on several occasions. The EDPS recalled some key elements, such as the need to take the time for reflection before rolling out new proposals without an assessment of the existing reality. He also addressed the issue of profiling which, while useful in some contexts, calls for appropriate safeguards in view of the potential intrusion in the private lives of citizens.

### 3.6.4. Conference on data protection and law enforcement (Trier)

On 26 and 27 May 2008, the EDPS and the European Law Academy (ERA) jointly organised a conference in Trier on data exchange and data protection in the area of freedom, security and justice. This seminar gave an overview of the relevant EU legislation. The analysis and discussion focused on key documents on data exchange, such as the Treaty of Prüm and the most recent decision on integrating it into the EU legal framework. In the field of data protection, the seminar dealt in particular with

the framework decision on data protection in the framework of police and judicial cooperation in criminal matters.

Other topics covered the increasing role in law enforcement of data collected by private companies (airlines, banks, telecoms operators), technological developments that facilitate the collection of data, as well as the institutional framework for data protection. A final session dealt with the future, under the Lisbon Treaty.



EDPS participation to ICT 2008 conference (Lyon, 25-27 November 2008).

The conference attracted around 100 participants from a large number of EU Member States. Specialists on data protection and law enforcement discussed the legal framework for data exchange and data protection, at present and in the near future. Many interventions underlined the importance of bringing together the perspectives of data protection and law enforcement, both necessary elements of good governance.

### 3.6.5. EU RTD

The EU Research and Technological Development (RTD) efforts constitute a very early and efficient step where privacy and data protection principles can be addressed, introduced and promoted driven by the concept of privacy by design. In 2008, the EDPS clarified and organised his possible contributions to the EU RTD and consolidated actions already initiated.

The EDPS's contributions to a research framework programme and to calls for proposals include the following:

- participation in workshops and conferences intended to identify future challenges that can be relevant for EU RTD policy;
- contribution to research advisory boards launched by the European Commission in

connection with the framework programme, and provision of opinions on data protection matters;

- assistance to the European Commission in the evaluation process of proposals, in particular regarding possible data protection issues these proposals might trigger.

The EDPS might also give an opinion in relation to individual RTD projects, either at the request of a consortium of a project, or on his own initiative.

### Policy paper on R & D

In April 2008, the EDPS adopted a policy paper — entitled 'The EDPS and EU research and technological development' <sup>(46)</sup> — describing the possible role the institution could play for research and developments (R & D) projects in the seventh framework programme for research and technological development (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.

<sup>(46)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28\\_PP\\_RTD\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf)

In November 2008, the EDPS ran a stand during the ICT 2008 event in Lyon which is considered to be Europe's biggest research event for information and communication technologies. The event gave the opportunity to present the EDPS's policy paper to some of the 4 500 registered delegates and to provide targeted support on the best possible ways they could handle data protection issues which might arise in their research activity.

Most of the possible EDPS contributions envisaged in the new policy paper have already been implemented during 2008 in the following actions:

- after having analysed the elements of the EU 'Turbine' project <sup>(47)</sup> (trusted revocable biometric identities) which aims at conducting research in the field of revocable biometrics, the EDPS decided to reply favourably to the consortium's request and will produce an opinion on the EU project in 2010;
- in the course of 2008 the EDPS decided to take a closer look into the ongoing Bridge (Building radio frequency identification for the global environment) <sup>(48)</sup> project. The EDPS sent recommendations to the European Commission based on the evaluation of a fact-finding step and a meeting with Commission staff in charge of the project. In the light of the EDPS's recommendations, the European Commission launched additional actions in order to clarify and increase conformity of the project's research activities with the community legislation on personal data;
- the EDPS provided and facilitated contact points of national data protection authorities to a series of consortiums of EU RTD projects during 2008. The aims of these requests were mainly to get further detailed information on the applicable data protection law and more appropriate contacts for possible notification of personal data processing.

#### European Commission research advisory groups

In order to follow the definition process of new EU RTD action lines more closely, the EDPS accepted to take part as an observer or intervene

on a case by case in the activities of the following research advisory groups managed by the European Commission:

- Riseptis (Research and innovation for security, privacy and trustworthiness in the information society): in 2008, the EDPS accepted an invitation from the Information Society and Media DG of the European Commission to join the group as an observer; this high-level advisory group in ICT research on security and trust aims at providing visionary guidance on policy and research challenges in the field of security and trust in the information society;
- ESRIF (European Security Research and Innovation Forum): ESRIF is a European strategy group in the civil security research domain that was established in September 2007. Its main objective is to develop a mid- and long-term strategy for civil security research and innovation through public-private dialogue by 2009. The EDPS intervened in a meeting of an ESRIF subgroup related to innovation issues;
- the EDPS also punctually intervened in European Commission's advisory groups dealing with 'Trusted computing' as well as future ubiquitous information society.

#### 3.6.6. Google / DoubleClick Merger and data protection issues

In March 2008, the European Commission cleared under the EU merger regulation the acquisition of the company DoubleClick — a company providing online advertising technology — by Google, the owner of one of the major Internet search engines. These companies manage vast databases containing personal data on both the searching and the surfing behaviour of Internet users. The combined use of these databases raises delicate and complex issues relating to the right to the protection of personal data.

At the end of January 2008, the EDPS contributed to a hearing organised by the Parliament's LIBE Committee on data protection on the Internet. Furthermore, as an advisor to Community institutions on all matters relating to data protection, the EDPS exchanged letters with European Commissioner for Competition Neelie Kroes. His staff met with the relevant staff at the Commission

<sup>(47)</sup> <http://www.turbine-project.eu>

<sup>(48)</sup> <http://www.bridge-project.eu/>



and provided expertise on data protection issues that may arise in competition cases such as this merger.

In this context, the EDPS welcomes that the Commission explicitly clarified in a press release that its decision is based exclusively on the EU merger regulation and is without prejudice to the merged entity's obligations under the EU and national data protection legislation.

Furthermore, the EDPS, as a member of the Article 29 Data Protection Working Party, actively contributed to a paper on data protection and search engines, which was adopted by the working party in April 2008.

### 3.6.7. Participation in expert groups

#### Radio Frequency IDentification (RFID) Stakeholders

By Commission decision of 28 June 2007, the expert group on radio frequency identification was set up<sup>(49)</sup>. This group is also known as the RFID-Stakeholders Group. In accordance with Article 4(4)(b) of the decision, the EDPS participates in the activities of the group as an observer. During the four meetings of the group which were organised in 2008, the EDPS participated in the discussions which aimed at contributing to a forthcoming recommendation to be issued in 2009. Within the group, the EDPS also contributed to the analysis conducted on the nature and the effects of the ongoing move towards the 'Internet of things' which resulted in the publication of a Commission staff working document in September 2008<sup>(50)</sup> and which will be the subject of a communication published later in 2009.

#### Data retention experts' group

The 'Platform on electronic data retention for the investigation, detection and prosecution of serious Crime' is a group of experts set up by Commission decision on 25 March 2008<sup>(51)</sup>. The group is composed of representatives from Member States' law enforcement authorities, associations of the electronic communications industry, data protection

authorities, as well as members of the European Parliament, and the EDPS. The group of experts works as a consultative group<sup>(52)</sup>. It will facilitate the sharing of best practise, and contribute to the Commission's assessment of the costs and effectiveness of Directive 2006/24/EC (data retention directive), as well as the development of relevant technologies which may impact on the directive<sup>(53)</sup>.

The group had its first formal meeting on 28 November 2008 (it has met informally four times since 2007). Several papers on the technical and legal aspects of data retention are under discussion. The EDPS participates actively in the meetings and will continue providing support during 2009.

#### Credit Histories

The EDPS participates as an observer in the Commission's experts group on credit histories, which had its first meeting in September 2008. The group gathers experts from credit registers, national consumers associations, banks and data protection authorities (including the French and Finnish data protection authorities). The group will finalise a report in May 2009 on the need and conditions for the cross border exchange of credit information of individuals within the EU. Several aspects of the project raise privacy issues, such as the exact purpose of the exchange of information, and the quality of data to be transferred. Together with other data protection authorities represented, the EDPS has highlighted these issues in order to achieve the right balance in the forthcoming report of the experts group.

### 3.6.8. Maritime accidents

In November 2008, the EDPS provided upon request a targeted advice relating to the proposal for a directive establishing the fundamental principles governing the investigation of accidents in the maritime transport sector. The proposal was already adopted by the Commission in 2005, and had reached the third and final stage of the co-decision procedure — the Conciliation Committee. The request for advice came from the Parliament's rapporteur who was member of this Committee.

<sup>(49)</sup> Decision No 467/2007/EC (OJ L 176, 6.7.2007, p. 25).

<sup>(50)</sup> [http://ec.europa.eu/information\\_society/europe/i2010/docs/future\\_internet/swp\\_internet\\_things.pdf](http://ec.europa.eu/information_society/europe/i2010/docs/future_internet/swp_internet_things.pdf)

<sup>(51)</sup> Commission Decision 2008/324/EC (OJ L 111/11, 23.4.2008).

<sup>(52)</sup> See Article 2 of the decision.

<sup>(53)</sup> Recital 6 of the decision.

The EDPS received the different opinions of the Council and the European Parliament on a specific article in the proposal which dealt with the collection and possible disclosure of personal data. The subsequent advice of the EDPS has helped the Committee to reach an agreement on this subject. The EDPS expressed his appreciation for this consultation, as it was the first time that he was consulted at this stage of the legislative process.

### 3.6.9. Communicable diseases

Communicable diseases such as tuberculosis, measles and influenza, do not respect national frontiers and can spread rapidly. New diseases emerge and others develop drug-resistant forms. In addition, new scientific developments on the role of infectious agents in chronic conditions such as cancer, heart diseases or allergies are under investigation. In responding to these various issues the network on communicable diseases started work in 1999<sup>(54)</sup>. The communicable diseases network is built on work done with Member States and consists of two pillars: surveillance and an early warning and response system (EWRS). The EDPS made informal comments on the Commission decision amending Decision No 2000/57/EC on the early warning and response system for the prevention and control of communicable diseases.

### 3.6.10. The Community Customs Code and the Economic Operators and Registration number (the EORI number)

The European Commission submitted an informal consultation to the EDPS based on the draft amending Commission Regulation (EEC) No 2454/93 of 2 July 1993 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code (hereinafter 'the draft'). This was the first time that the EDPS was consulted in the frame of the adoption of a Commission regulation, where the Commission is assisted by a Committee (the Customs Code Committee, in this case). The

EDPS did not issue an opinion, but sent three advisory letters to the Commission.

The new instrument proposed a legal basis for a system of identification and registration of economic operators and other persons, enabling them to register only once for all their interactions with customs authorities throughout the Community. In order to store and exchange the registration and identification data of economic operators and also other persons between customs authorities and between the Commission and customs authorities, an electronic registration and identification system (EORI) will be established. Furthermore, the data from national systems will be consolidated at a central level and sent to Member States at regular intervals.

The EDPS advised the Commission on many aspects, in particular with regard to:

- the co-supervisory role of the EDPS and national data protection authorities;
- the difference between 'economic operators' and 'other persons' (data subjects) in what concerns the necessity and proportionality of the processing activity. This has an impact on the basis for lawfulness of processing, conservation period, etc.;
- the rights of the data subject, consent as the legal basis for publication of personal data on the Internet and the adoption of security measures.

## 3.7. New developments

### 3.7.1. Interaction with technology

The development and use of new technologies is expected to contribute to a qualitative change of society as a whole. These new perspectives have been characterised as 'ubiquitous information society', 'ambient intelligence space' or 'Internet of things'. Their sustainability will be secured only if the challenges, and in particular data protection and privacy issues, are appropriately addressed at the earliest stage of their development. A thorough analysis of the technological trends which drive the evolution of the European society into a European information society is a key success factor for fostering a crucially important trust in this emerging environment.

---

<sup>(54)</sup> Decision 2119/98/EC of the European Parliament and the Council.



Cloud computing integrates data silos and challenges the application of the data protection EU regulatory framework.

### Cloud computing

In the annual report 2007, the EDPS already raised serious concerns about not-yet-addressed privacy and security issues related to the development of cloud computing<sup>(55)</sup>. The need to implement appropriate safeguards in order to provide a sustainable development for this emerging technology is still unanswered. Simultaneously, more and more services supported by cloud computing facilities are proposed, not only to business or government users but also to individuals.

The principle of cloud computing presents a real challenge for a proper identification of the applicable law related to the processing of personal data,

<sup>(55)</sup> Cloud computing refers to the use of Internet ('cloud')-based computer technology for a variety of services. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure 'in the cloud' that supports them.

the responsible actors and other legal consequences involved. The following example illustrates the flexibility which could be offered by cloud computing, but also the issues it triggers for the enforcement of the EU legal framework. In order to lower energy cost, cloud-processing activities might be directed primarily to data centres, which are powered by solar energy and under the sun at the time of the request for processing; those located momentarily on the dark side of the Earth and functioning with other energy could be less accessed. Although environmentally attractive, this example also shows that it would be almost impossible to define where the processing will take place and by which actors of the cloud. It is also possible to envisage that personal data stored in third country data centres could be subject to subpoena and disclosed to the government of the jurisdiction where the cloud computing servers are located.

One possible solution which has already been suggested would be to force personal data to be processed

and stored only in 'EU cloud' servers which are physically located on the EU territory and under the EU data protection regulatory framework. But this constraint would go against the foundations of a promising technology and the great flexibility and adaptability cloud computing is supposed to offer. It also seems to disregard that the EU data protection framework currently applies *regardless* of where the data are being processed, as long as the processing is carried out in the context of the activities of an establishment of the controller in the EU or the means used are situated there (see Article 4 of Directive 95/46/EC). However, it is true that the uncertainties presently involved in cloud computing are raising new challenges for an effective implementation and enforcement of data-protection standards.

Data could of course be encrypted before being sent into the cloud, but again that would jeopardise large processing facilities offered by cloud computing as this data cannot be processed as soon as it is encrypted<sup>(56)</sup>. Yet, greater awareness among the key actors of the risks involved and the responsibilities for addressing them both adequately and effectively will be an important condition for generating trust in these new environments.

### **DNA sequencing**

As a result of a huge R & D effort produced in the frame of the human genome project<sup>(57)</sup>, human genes were successfully and almost completely sequenced in 2001. Around 3 billion pair bases and between 20 000 and 25 000 genes have been located and identified.

The goal of the Archon X Prize for Genomics<sup>(58)</sup> will still require a couple of years to be reached. However, numerous private entities have mushroomed in the field of genetic testing and already propose genetic-analysis targeting identification of specific traits and possible diseases for less than EUR 400.

---

<sup>(56)</sup> See the papers of Carl Hewitt, Emeritus at Massachusetts Institute of Technology (<http://carlhewitt.info/>).

<sup>(57)</sup> [http://www.ornl.gov/sci/techresources/Human\\_Genome/home.shtml](http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml)

<sup>(58)</sup> This prize will be awarded to the first team that can build a device and use it to sequence 100 human genomes within 10 days or less at a cost which will not exceed USD 10 000 per genome (<http://genomics.xprize.org/>).

This extremely rapidly growing industry is mainly supported by the following technological trends:

- the growing availability of huge processing capability required for the analysis of massive amounts of data which is fostered by the development of interconnected data centres;
- the spin-offs and DNA analysis breakthroughs generated by the human genome project;
- other technological trends already described in previous EDPS annual reports which are an unlimited band width and unlimited data storage capacity.

The genetic analysis services offered by these companies rely on the scientific accuracy of links they establish between the data subject's genetic information and possible related traits or diseases. These causal links are built on numerous elements like statistical analysis, availability of R & D reports, which can be summarised by the ability of these companies to have access to reliable large databases of scientific information.

As recently highlighted by a decision of the European Court of Human Rights in a case about the use of DNA for law enforcement purposes<sup>(59)</sup>, genetic samples can reveal 'much sensitive information about an individual, including information about his or her health' and therefore need to be processed with the highest privacy and data protection safeguards.

Increasingly, genetic analyses are offered through the Internet and therefore open to anybody inside and outside the country where the company is based. These tests, whose availability was previously primarily limited to a strongly regulated medical and judicial field, are now offered on a commercial scale. The DNA sample which is analysed does not necessarily belong to the person who sends it, but could be submitted by anybody who was able to collect this sample.

The promising light-speed DNA-sequencing technology and its borderless availability will, if not appropriately handled, challenge the traditionally

---

<sup>(59)</sup> Case of S. and Marper v. the United Kingdom, 5 December 2008.

implemented safeguards restricting the access to the most sensitive personal data and raise critical privacy issues.

### 3.7.2. New developments in policy and legislation

#### Lisbon Treaty

In 2008, reflections started on the consequences of the entry into force of the Lisbon Treaty. In this context, the EDPS took stock of the consequences of the new treaty for data protection, such as the new legal basis for data protection (Article 16 of the Treaty on the Functioning of the European Union), as well as of the abolishment of the pillar-structure. As a result of the rejection of the Treaty by Ireland on 12 June 2008, these activities were not pursued. At present, there are new perspectives of a possible entry into force of the Lisbon Treaty at the end of 2009 or early 2010.

#### Commission legislative and work programme for 2009 and the Stockholm programme

The Commission legislative and work programme for 2009 took a focused approach and concentrated on a limited number of new policy initiatives. Within this approach, there was much emphasis on impact assessments before the Commission presents a proposal as well as on the review of existing EU legislation and pending proposals.

This approach is also reflected in the way the Commission envisages proceeding in the area of freedom, security and justice. The Commission legislative and work programme for 2009 mentioned the completion of the Hague programme for freedom, security and justice (from November 2004), as well as further steps towards a common policy on migration. A central development in the Commission programme is the foreseen new multi-annual programme in the area of freedom, security and justice to be adopted under the Swedish Presidency of the Council (often referred to as the Stockholm programme). In the report of the so-called 'Future group', the balance between mobility, security and privacy was given a central place. This report, together with the principle of convergence introduced in the report, will be a building block for the Stockholm-Programme.

#### Major trends in law enforcement

The inventory for 2007 noted as a major trend the legislative activities relating to the combat of crime, and in particular the fight against terrorism and organised crime. This trend continued in 2008.

Moreover, new legal instruments were proposed as an addition to existing legal instruments, which have not yet been fully implemented. This raised questions relating to the necessity of such new instruments, instead of focussing on the practical implementation of existing instruments. This issue will be addressed by the EDPS in his further input in the discussions on the EU-PNR proposal.

Finally, a continuing trend in 2009 will be the opening up of existing databases (European databases, as well as national databases) for law enforcement, despite the fact that the original purpose of the database is a different one. Related issues are the interoperability and interconnection of databases, as well as activities relating to profiling of persons.

#### Data Protection Framework Decision

In the legislative field, the adoption of Council Framework Decision 2008/977 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters meant that, for the first time, a general legal framework for data protection in this area was established on the level of the EU. However, the framework decision does not apply to all relevant situations and other instruments for data protection in this area are still in place.

Throughout the negotiations, this piece of legislation has been a major focus of attention for the EDPS, who issued three opinions as well as comments on the subject. The EDPS's opinions acknowledged the initiative as a considerable step forward for data protection in police and judicial cooperation, and as a necessary complement to other measures introduced to facilitate the cross-border exchange of personal data in law enforcement. At the same time, the EDPS repeatedly called for significant improvements of the proposal to ensure high standards in the level of protection offered and warned against a dilution of data protection standards. In particular, he regretted that the framework decision only

covers police and judicial data exchanged between Member States, EU authorities and systems, and does not include domestic data.

Further steps are therefore needed — either under the Lisbon Treaty or not — to increase the level of protection provided by the new instrument. The EDPS therefore encourages the Community institutions to start the reflections on further improvements of the framework for data protection in law enforcement as soon as possible.

#### **Future of the data protection directive**

At different levels discussions take place on the future of Directive 95/46/EC. These discussions focus on the implementation of the directive, not excluding the possibility of a future modification of the directive. The ongoing review of the directive may offer the opportunity to reflect on the need for modifying this directive in order to ensure its continued effectiveness or for adopting specific rules to address data protection issues raised by new information and communication technologies.

Many activities have already been started and will be completed in 2009. Besides the activities of the Article 29 Working Party, the following activities can be mentioned.

- The Commission has announced a public consultation on the directive, including a conference of all stakeholders in May 2009.
- Last year, the UK Information Commissioner's Office (ICO) invited tenders to assess the strengths and weaknesses of the EU data protection law and to recommend updates that relieve the bureaucratic burden it entails. The study will examine the EU data protection directive and its application to identify better ways to provide effective protection for individuals and society and minimise burdens on organizations. The study is intended for discussion at the annual spring conference of European data protection commissioners in April 2009 and for publication in May 2009. Although only the European Commission can initiate the process for changing the directive, the

ICO wants to start a debate about the strengths and weaknesses to ensure that EU data protection law effectively meets the needs of organisations and individuals.

#### **Public health**

The EU has an ambitious programme with the purpose of improving citizens' health in the information society, where the EU sees great possibilities for enhancing cross-border healthcare through the use of information technology. Public health is a new area of attention for the EDPS. The emphasis will be put on health information systems, the development of e-health systems, the secondary use of medical data, the question how to deal with legislative activity relating to sensitive information and some other fundamental questions, also relating to criticism in the medical sector about data protection law.

It goes without saying that enhancing cross-border healthcare, in combination with the use of information technological developments, has great implications for the protection of personal data. A more efficient and therefore increasing exchange of health data, the increasing distance between persons and instances concerned, the different national laws implementing the data protection rules, lead to questions on data security and legal certainty. The principle of traceability will play an important role.

#### **Other**

In 2009, the EDPS will focus on a few specific areas of EU action:

- the relation between data protection and the collection and use of statistics;
- activities relating to public access to documents, such as the modification of public access Regulation (EC) No 1049/2001.

Finally, special attention will be given in 2009 to how to advise the Commission in cases where it does not adopt a proposal (to the Council and/or the European Parliament) but decides itself.

## 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>(60)</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) 45/2001 provides that the EDPS participates in the activities of the working party.

<sup>(60)</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.

The EDPS considers this to be a very important platform for cooperation with national supervisory authorities. It is also evident that the working party should play a central role in the uniform application of the directive, and in the interpretation of its general principles.

In February 2008, the working party adopted a new bi-annual work programme <sup>(61)</sup>. It decided to concentrate on four main strategic themes and a few topical issues which it found most relevant and urgent for the development of data protection.

The working party identified three major challenges:

- how to improve the impact of Directive 95/46/EC and the role of the working party;
- the impact of the new technologies;
- the global environment (international transfer of data, global privacy and jurisdiction).

The main strategic themes, developed in more detail in the work programme, are therefore:

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

<sup>(61)</sup> Work programme for 2008-09, adopted on 18 February 2008 (WP 146).

Further to this work programme, the working party already made important progress along these lines in several areas:

- international transfers: a package of working documents to facilitate the use of binding corporate rules (BCR) (WP 153-155) and ongoing monitoring of PNR issues (WP 151);
- new technologies: Opinion 1/2008 on data protection issues related to search engines (WP 148) and Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (e-privacy directive) (WP 150);
- making the working party more effective: mandate for a second joint investigation into compliance at national level with data protection requirements in the context of traffic data retention (WP 152);
- better implementation of Directive 95/46/EC: work is ongoing on the concepts of ‘data controller’ and ‘data processor’ and on the issue of ‘applicable law’.

The working party also ensured a close follow-up to developments with regard to EU border management, security and border control (US ESTA), and biometrics and visa applications.

In this context, the working party also took position on proposals for legislation or similar documents. In some cases, these subjects had been dealt with in opinions of the EDPS on the basis of Article 28(2) of Regulation (EC) No 45/2001 (see Chapter 3). The EDPS’s opinion is a compulsory feature of the EU legislative process, but contributions of the working party are also very useful, particularly since they may contain special points of attention from a national perspective. The EDPS therefore welcomes these contributions which have been consistent with his own opinions.

More in general, the EDPS and the working party have closely cooperated in good synergy on a range of subjects, but especially focussing on implementation of Directive 95/46/EC and on challenges raised by new technologies. The EDPS also strongly supported initiatives taken to facilitate international data flows (BCR).

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 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. As a result, two meetings were held during the first half of 2007. The Portuguese Presidency provided for one additional meeting, but it was cancelled.

The Slovenian Presidency convened one meeting of the working party in May 2008. During this meeting the Assistant EDPS presented the EDPS’s opinion on the review of the e-privacy directive, the EDPS’s 2007 annual report and the EDPS’s priorities for consultation on proposals for new legislation in 2008.

There was also an exchange of views on Directive 95/46/EC, mainly based on a number of topics, such as the relation of data protection under the directive and the freedoms of information and expression; the need for specific provisions with regard to technical developments (new risky technologies), and simplification of notification and



information requirements (especially for small and medium-sized enterprises).

The outcome of this exchange of views was that there seemed to be general satisfaction with Directive 95/46/EC. However, there was also a general need for further discussion after an eventual ratification of the Treaty of Lisbon.

The working party did not meet under the French Presidency, but the Czech Presidency has again provided for one meeting in March 2009.

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 (see Section 2.8) has developed rapidly since its start, only a few years ago.

The Eurodac Supervision Coordination Group (hereinafter ‘the group’) is composed of representatives of the national data protection authorities and the EDPS, and met twice in 2008, namely in June and in December. The focus of this year has been to implement the work programme adopted by the group in December 2007.

At the same time, the framework in which the group is operating has also attracted attention; the Commission has undertaken the review of the Dublin and Eurodac regulation, in the framework of the asylum measures in general <sup>(62)</sup>.

In order to get information from various stakeholders, the European Parliament’s LIBE Committee organised on 29 May 2008 a round table on ‘The Dublin system — where are the gaps, what are the alternatives?’. The EDPS had an opportunity to

present some views on this issue and underlined *inter alia* how the coordinated supervision of Eurodac could play a role in improving the system.

The group is aware of these evolutions and is willing to contribute to the development of the new instruments by sharing and assessing experiences at national level.

#### Activities of the group in 2008

At the meeting in June 2008, and as foreseen in Article 3 of its Rules of Procedure, the group has elected a chairperson and a vice-chairperson. There were two candidates: Mr Peter Hustinx (EDPS) for Chair and Mrs Guro Slettemark (DPA Norway) for vice-chair. The two candidates have been elected by the unanimity of the votes validly cast.

At the December 2007 meeting, the group had selected within the work programme three subjects for closer examination and reporting. The group has been focusing on these three topics in 2008, working first at national level on the basis of standard questionnaires. The aim is then to compile and analyse answers, in order to provide guidance, where appropriate and useful.

#### • Information of the data subjects

The coordinated inspection report issued in 2007 suggested as a probable cause for the scant exercise of the right of access a lack of awareness of data subjects about their rights. The group has decided to examine the way information is provided to asylum seekers or persons otherwise reported in Eurodac. The purpose of this exercise is to identify and exchange best practices in this matter (which languages are used, is the impact of the information measured in any way, and similar issues).

#### • Children and Eurodac

According to Article 4 of the Eurodac regulation, children from 14 years on should be fingerprinted. There is often a problem determining the age of a child who has no reliable identity document. The group will address the question of the rules and methods established by the national Eurodac authority to determine if the applicant is underage

<sup>(62)</sup> On 3 December 2008, the European Commission tabled several proposals ‘to strengthen the rights of asylum seekers in the Union’. This package of measures contains three proposals, aiming at reviewing refugee reception conditions in the EU, the Dublin II regulation and the Eurodac regulation, which set up the Eurodac database.

and examine whether the rules comply with the United Nations Convention on the Rights of the Child.

The national inspections on these two topics have been launched in August 2008. The report on both is expected by mid-2009.

- **DubliNet** <sup>(63)</sup>

As a third topic to address in a coordinated inspection, the group opted for the use of DubliNet and in particular data security issues in that context. The group will examine the following questions: What are the rules of exchange of data through DubliNet at national level? What are the measures taken to ensure the protection of personal data in that exchange of information? How is further use regulated?

For all these topics, the work of the group appears very timely in view of the revision of the Eurodac and Dublin regulations. The reports produced by the group should contribute usefully to the review of the texts.

Finally, the rules of procedure of the group have been revised in December 2008 due to the adoption by the EDPS of new rules for reimbursement of travel expenses, which may also cover daily allowances. This required a modification of the internal rules of the group.

#### 4.4. Third pillar

The need for close cooperation between the EDPS and other data protection authorities in the area of police and judicial cooperation has acquired an increasing importance over the last years by virtue of many EU and international initiatives aimed at collecting and sharing personal data, sometimes through the creation and interconnection of databases.

First of all, 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' (Article 46(f)(ii) of Regulation EC (No) 45/2001). 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 and are supported by a joint data protection secretariat in the Council of the European Union.

Furthermore, the EDPS cooperates with national data protection authorities, in particular by contributing to the Working Party on Police and Justice (WPPJ), to which the European conference conferred the mandate to monitor the developments in the area of law enforcement with regard to the processing of personal data, to prepare all necessary actions to be taken by the conference in this area, as well as to act on behalf of the conference when a quick reaction is urgently needed.

The EDPS actively contributed to the meetings held by the WPPJ during 2008. In many cases, the EDPS contributed to the debate by presenting his opinions or by participating in subgroups. The EDPS was also invited to deliver a presentation on the changes that the Lisbon Treaty would bring about, especially with regard to the area of police and justice cooperation. The WPPJ addressed various and delicate issues that included the following:

- with regard to the implementation of the Prüm Treaty in the EU legal system, the WPPJ sent a letter to the Chair of the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament and adopted a position paper on the detailed rules and standards contained in the annex to the main proposal. In these documents, the working party emphasised, along the lines put forward by the EDPS in his opinions, the lack of a solid general framework for data protection in the third pillar and called for clear rules concerning independent supervision, purpose limitation and transfers to third countries;
- with regard to the negotiations on the framework decision on data protection in the third pillar, the WPPJ voiced concerns on its limited

---

<sup>(63)</sup> DubliNet is the secure electronic network of transmission channels between the national authorities dealing with asylum applications. Usually, a 'hit' in the Eurodac system will trigger an exchange of data about the asylum seeker. This exchange will use DubliNet.

scope of application as well as on the lack of an advisory forum of national and European supervisory authorities to ensure the harmonised application of its provisions;

- the WPPJ also dealt with the issue of passenger name records (PNR), in conjunction with the Article 29 Working Party, and contributed to the discussion launched by the European Commission on the new multi-annual programme in the area of freedom, security and justice.

#### 4.5. European conference

Data protection authorities from Member States of the EU and the Council of Europe meet annually for a spring conference to discuss matters of common interest and to exchange information and experience on different topics. The EDPS and Assistant EDPS took part in the conference in Rome on 17 and 18 April 2008, hosted by the Italian data protection authority (*Garante per la protezione dei dati personali*), under the general theme ‘What outlook for privacy in Europe and beyond?’.

The conference dealt with various developments related to security and new technologies. A focus on border management was visible in a declaration<sup>(64)</sup> adopted by the conference on three communications of the European Commission on this subject. It called for evaluation of the effectiveness of existing measures, before embarking on new measures limiting the rights and freedoms of travellers. However, the conference also looked into very practical subjects, such as the protection of children’s data and the Portuguese experience with raising awareness in schools. The EDPS intervened on new challenges for the data protection community and the opportunities provided by the Lisbon Treaty.

Just before the conference, a workshop was held to take stock of developments in the context of the London initiative (see Section 4.7) and to share results with most European colleagues.

The next European conference will be held in Edinburgh on 23 and 24 April 2009, and focus on the experience with Directive 95/46/EC.

<sup>(64)</sup> Available at EDPS’s website, Section Cooperation, under European Conference.

Staff members participated in case handling workshops in Ljubljana and Bratislava in March and September 2008. This interesting mechanism of cooperation at staff level — for exchange of best practices among European DPAs — is now in its 10th year. The next case handling workshop will be held in Prague in March 2009.

#### 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 30th International Conference of Data Protection and Privacy Commissioners was held in Strasbourg from 15 to 17 October 2008 and hosted jointly by the French Data Protection Commission (CNIL) and the German Federal Commissioner for data protection and freedom of information, in close cooperation with the Council of Europe. It was attended by a large number of delegates from some 60 countries around the world.

The conference with the general theme ‘Privacy in a borderless world’ provided for six plenary sessions in the hemicycle of the Council of Europe — ‘Is privacy an obstacle or an asset for global economic growth?’; ‘Privacy, an endangered space?’; ‘Security towards a worldwide identification database?’; ‘My name is Clara, I am 14, here is my private life — my accomplishments’; ‘The digital-assisted man: a digital angel or a digital devil?’; ‘Limits and new instruments of regulation for the future of privacy?’. There was also a closed session for commissioners.

The EDPS and Assistant EDPS both attended the conference. The EDPS moderated the plenary panel on ‘Limits and new instruments of regulation’, and reported on the London initiative in closed session.

The conference concluded by stressing the need for binding data-protection rules in a globalised world. Without such international rules for all players, it will not be possible to tackle the privacy challenges of the future. Delegates called for increased international cooperation among data protection authorities and emphasised that data protection must play a



International conference of data protection and privacy Commissioners (Strasbourg, 15-17 October 2008).

more prominent role in the policies of public and private institutions. Individuals have to be provided with appropriate means for the protection of their privacy.

The conference adopted various resolutions on new technologies or the need for international dialogue <sup>(65)</sup>:

- Resolution on children’s online privacy;
- Resolution on privacy protection in social network services;
- Resolution to explore establishing an international Privacy/data protection day or week;
- Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a joint proposal for setting international standards on privacy and data protection.

The conference also provided for the establishment of a steering group on representation of the international conference at meetings of international organisations.

<sup>(65)</sup> Available at EDPS’s website, Section Cooperation, under International Conference.

The next international conference will be held in Madrid from 11 to 13 November 2009 and hosted by the Spanish data protection authority, *Agencia de Protección de Datos*.

#### 4.7. London initiative

At the 28<sup>th</sup> 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>(66)</sup>.

In the context of the London initiative, a number of workshops have taken place to exchange expe-

<sup>(66)</sup> See Annual report 2006, paragraphs 4.5 and 5.1.

rience and share best practices in different areas, such as communication, enforcement, and strategic planning.

In May 2008, the Canadian Privacy Commissioner hosted a workshop in Montreal devoted to management issues in data protection authorities. This was the first occasion to jointly look into management of human resources (training and expertise), financial resources (funding models) and ensuring effectiveness (operational management and management structure) as well as management of external relationships (privacy officers, civil society and regional networks).

In October 2008, the EDPS presented an overview of the London initiative's state of play for the closed session of the 30th international conference in Strasbourg.

The organisation of workshops for the exchange of best practices is likely to continue in 2009 on 'how to respond to security breaches'.

#### 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 is collected or exchanged between organisations. The international conference addressed this in a

resolution in Sydney in 2003, calling for 'international and supra-national 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 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.

A third workshop is presently under consideration. It is likely to be organised at the end of 2009 or early in 2010 and will inter alia deal with the responsible use of biometrics in various contexts.

## 5. Communication

### 5.1. Introduction

Information and communication play a pivotal role in ensuring visibility of the EDPS's main activities and in raising awareness both of the EDPS's work and of data protection in general. This is all the more strategic since the EDPS is still a relatively new institution and, therefore, awareness of its role at EU level needs to be further consolidated.

If we look back to the period spanning from the EDPS's very first year of activity to 2008 — the last year of the first mandate — we can take full measure of all the progress made so far. Increasing the EDPS's visibility on the EU political map was the clear focus of the EDPS's 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. Expanding on the generically elaborated methods of the first year, an information strategy was developed along the usual lines: creation of a clearly identifiable house style (logo, visual identity), definition of general and specific objectives, identification of key audiences in relation to the main activities of the EDPS (see Section 5.2), and selection of communication tools that should be commensurate with each considered target group. Subsequent work was primarily devoted to the development of a set of communication tools and practices which are customary for most public bodies (e.g. website, newsletter, brochures, background papers, speeches and participation in conferences, press releases, press conferences, organisation of awareness-raising events). A press service was concurrently established to deal

with external communication via the media (see Section 5.4).

Five years after the start of work, we can see that the emphasis placed on communication, including a targeted approach and the development of information and communication tools and channels, generated payoff in terms of visibility. Meaningful indicators of achievements include in particular a higher volume of requests for information and advice, increased traffic on the website, a constant rise in the number of subscribers to the newsletter, as well as regular requests for study visits at the EDPS's premises and invitations to speak at conferences. Similarly, more systematic contact with the media and, as a result, substantial rise in media coverage of EDPS's activities further emphasise the view that the EDPS has become a point of reference for data protection issues.

The increased visibility of the EDPS in the institutional landscape is of immediate relevance for his three main roles: i.e. the supervisory role in relation to all Community institutions and bodies involved in the processing of personal data; the consultative role in relation to those institutions (Commission, Council and Parliament), that are involved in the development and adoption of new legislation and policies that may have an impact on the protection of personal data; and the cooperative role in relation with national supervisory authorities and the various supervisory bodies in the third pillar.

A specific aspect of data protection awareness in the supervisory role is the cooperation between the EDPS and data protection officers (DPOs) in Community institutions and bodies. Close

cooperation with DPOs is an important method of sharing good practices and effectively working together to build awareness on data protection issues among EU stakeholders and EU staff. The EDPS is eager to push this cooperation further, notably by encouraging joint actions and synergies, for instance in the context of the organisation of awareness-raising events, such as the annual Data Protection Day, on or around 28 January.

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

Another interesting initiative at the interface of better communication and more effective data protection is the EuroPrise project designed to test the feasibility of a European privacy seal for privacy-compliant goods and services. This project has been successfully developed by the 'Independent Centre for Privacy Protection Schleswig-Holstein', the regional data protection authority in Kiel (Germany), with a number of other stakeholders, among which several other national or regional data protection authorities in Europe.

The EDPS was able to attend the 30th anniversary of data protection in Schleswig-Holstein in July 2008, and on that occasion also presented the first European privacy seal to a company for the development of a 'privacy friendly' search engine. This was also intended as a general endorsement of the European privacy seal as an important and welcome mechanism to promote 'privacy compliant' IT products and services. The EDPS was also involved in the presentation of three more European privacy seals at a EuroPrise workshop in November 2008 in Stockholm <sup>(67)</sup>.

<sup>(67)</sup> See: 'Data Protection in Schleswig-Holstein, in Europe and in a Global Information Society', Kiel, 14 July 2008, and 'Introductory remarks on Presentation of European Privacy Seals', Stockholm, 13 November 2008, speeches available at EDPS's website.



EuroPrise, award of the first European Privacy Seal (Kiel, 14 July 2008)

The EDPS sees the European privacy seal as a particularly creative and promising instrument to promote and ensure an effective protection. On the one hand, it fits well with the key notion of 'privacy by design' as an effective means to ensure 'privacy compliant' and where possible even 'privacy enhancing' IT products and services. On the other hand, it offers a clear incentive for developers and providers of such products and services to invest in better privacy protection and benefit from these investments where this is justified. This is also to the clear benefit of users and all others who have a right to make an informed decision in these matters.

The following parts of this chapter describe the activities of the EDPS in 2008 in the area of information and communication, which encompassed participation of the EDPS in conferences and workshops, the work of the press service and external communication with the media, the processing of information requests, the development of online information tools (website and newsletter) and publication materials, study visits and the organisation of awareness-raising events.

## 5.2. Communication 'features'

The EDPS's 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. This requires a tailor-made approach using the most appropriate tools to target the right audiences, whilst at the same

time being adaptable to a number of constraints and requirements.

### **Key audiences and target groups**

Unlike most other EU institutions and bodies, whose communication policies and activities need to operate on a general level, addressing EU citizens as a whole, the EDPS's direct sphere of action is much more distinct. It is primarily focused towards Community institutions and bodies, data subjects in general and EU staff in particular, EU political stakeholders, as well as 'data protection colleagues'. Therefore, the EDPS's communication policy does not need to engage in a 'mass communication' strategy. Instead, awareness around data protection issues among EU citizens in the Member States essentially depends upon a more indirect approach, mainly via data-protection authorities at national level, and the use of information centres and contact points.

The EDPS however 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's office for instance) and participating in public events, meetings and conferences.

### **Language policy**

The EDPS's communication policy also needs to bear in mind the specific 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. Constant efforts are therefore made for that purpose, also with the aim of correcting the excessive 'legal' image of data protection.

When considering more specialised audiences (e.g. the media, data protection specialists, EU stakeholders), technical and legal terms 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's communication style follows along the lines of 'too much information kills information', thereby prompting to avoid 'over-communication'. The use of 'traditional' communication tools such as press releases 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.

Measuring the effects of communication activities is also decisive in order to assess the effectiveness of the approach followed and, where necessary, to reorientate the action. With this in mind, a review of the information strategy that was put in place following the establishment of the EDPS will be carried out in 2009.

## **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 21 January, he intervened at a public seminar on the merger of Google and Double Click. On 11 February, he commented on the draft framework for third pillar data protection. On 26 March, he presented his opinion on security features and biometrics in passports, and continued with a summary of his annual report for 2007. On 5 May, he presented his opinion on the revision of the e-privacy directive. On 29 May, he contributed to a round table on the Dublin asylum system in relation with the coordinated supervision of Eurodac. On 2 June,





Peter Hustinx delivering a speech at the International conference of data protection and privacy Commissioners (Strasbourg, 15-17 October 2008).

he spoke at a hearing on public access to documents. On 30 June, he made two contributions to a round table on external borders. On 8 September, he presented additional comments on the revision of the universal service and e-privacy directives.

The EDPS also appeared in other meetings with the European Parliament. On 26 February, he spoke in the Employment Committee on social security issues. On 14 May, he addressed a meeting of the Secretary General and the Directors General of the Parliament on compliance with Regulation (EC) No 45/2001. On 17 September, he discussed various issues related to the revision of the e-privacy directive with MEPs from different committees and political groups. On 6 November, he spoke at a seminar of the Parliament's legal service about recent issues at the interface of first and third pillar.

On 25 March, the EDPS presented his opinion on the EU PNR proposal in the Council's multidisciplinary group on organised crime. On 11 September, he appeared in the group for a second time to comment

on strategic issues presented by the French Presidency. On 30 September, he spoke at a conference on security research in Paris organised in the framework of the French Presidency. On 6 October, he contributed to a similar conference in Nice on the 'Internet of Things'. On 11 December, he spoke at a seminar on public access to documents organised by the Finnish permanent representation in Brussels.

Other EU institutions were also on the list. On 24 April, the EDPS and Assistant EDPS made a visit to the Civil Service Tribunal in Luxembourg for a briefing on relevant data protection issues. On 12 June, the 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 17 December, the EDPS and the Assistant EDPS both intervened at an EDPS seminar in Brussels with stakeholders on the supervision of EU institutions

On 25 January, the EDPS gave a lecture at the College of Europe in Bruges on 'Protecting personal

data in the EU: Principles, players and challenges'. On 26 May, he contributed to a conference on third pillar data protection at the European Law Academy (ERA) in Trier. On 10 June, he visited the European University Institute in Florence and delivered a lecture about 'EU data protection in a global economy: Threats and dangers to collective security and human rights'.

At the end of January, the EDPS was in the US for a programme of meetings with federal officials and other privacy stakeholders. On 28 January, he contributed to a conference at Duke University in Durham, North Carolina (USA) to celebrate 'Data Privacy Day'. On 29 January, he spoke at Georgetown University in Washington DC. On 30 January, he gave a lecture at the American University's Washington College of Law in Washington DC. On 31 January, he spoke at a meeting organised by the European Institute in Washington DC.

The EDPS also had various meetings with members of national parliaments. On 5 March, he testified before a committee of the House of Lords on the surveillance society in London. On 20 March, he took part in a seminar on privacy issues organised by the Justice Committee of the Dutch Senate. On 2 April, he appeared before a subcommittee of the House of Lords on EU PNR in Brussels. On 4 April, he spoke at the sixth Parliamentary Colloquy Paris–Berlin 'Collective security and individual liberties' in Lyon on ensuring a right balance between security, mobility and privacy.

In the course of the year, the EDPS also visited different Member States on other occasions. On 23 January, he spoke at a conference on biometrics at the Institute for Political Science in Paris. On 15 February, he appeared before an advisory committee of the Dutch government on security and privacy in The Hague. On 3 March, he spoke at a conference for law school students at Erasmus University in Rotterdam. On 28 April, he presented his policy paper on 'EU research and technological development' at the Institute for Technology Assessment in Vienna. On 6 May, he spoke at the ninth Data Protection Conference in Berlin about 'Strategic challenges for data protection in Europe'. On 28 May, he took part in

a panel discussion at the International Chamber of Commerce in Paris. On 6 June, he delivered a speech on road tolling at a conference on Intelligent Transport Systems in Geneva. On 20 June, he gave a speech on EU data protection at the Hungarian DPA in Budapest. On 14 July, he attended the 30th anniversary of data protection in Schleswig-Holstein and delivered a speech in Kiel (see also Section 5.1).

On 16 September, he spoke at a corporate counsel summit in Geneva. On 23 September, he took part in a public debate on privacy issues in Amsterdam. On 25 September, he gave a speech at a conference of the American Bar Association's international section in Brussels. On 11 October, he contributed to a Challenge conference on security and privacy in Paris. On 22 October, he spoke at the conference Biometrics 2008 in London. On 27 October, he spoke at an RSA conference on security breach and e-privacy issues in London. On 2 December, he presented at a conference on border management in Brussels. On 3 December, he spoke about 'proportionality' at a justice conference in London. On 9 December, he spoke about privacy and security research at an ESRIIF subgroup meeting in Ispra.

The Assistant EDPS made similar presentations. On 11 April, he made a presentation on the incidence of data protection on the judicial proceedings in the *Centre d'Estudis* of the Catalan Government. On 6 May, he spoke about the tensions between security and data protection at an international seminar organised by the Catalan data protection authority. On the same date in Barcelona, and on 7 May in Madrid, he delivered a speech on the forthcoming possible changes in data protection EU directives before a group of legal counsellors. On 20 May, in Madrid, he delivered a presentation at a training seminar for judges and public prosecutors on the impact of data protection in the context of civil proceedings. On 22 May, he spoke about the new framework decision on data protection in an international seminar for judges and public prosecutors in Toledo.

On 9 September, in Budapest, he addressed the annual conference of European companies specialised in data destruction on the topic of conservation, erasure and security measures about personal

data. On 4 October, he presented the new European criminal record information system (ECRIS) at the annual conference of the European Criminal Bar Association, in Bratislava. On 7 October, he made a presentation of the future challenges for data protection at a seminar organised by the ALDE Group in the European Parliament, in Brussels. On 28 October, he spoke on medical data at a meeting of the public health network of Andalucia, in Granada. On 25 November, he delivered a presentation on the impact of new technologies in the field of security in a seminar of the Centre for European Policy Studies (CEPS) in Brussels. On 3 December, he spoke at a workshop organised by the Superior Court of the Basque Country, in Bilbao, on data protection and judicial information. On 12 December, in The Hague, he spoke on the balance between security and data protection at the Seventh Annual Conference of the International Criminal Law Network.

## 5.4. Media relations

### Press service

The press service is in charge of the external communication with the media through regular contacts with journalists. It also deals with requests for information and advice coming from the press, interested parties or citizens, writing press releases and newsletters, as well as organising press conferences, study visits and interviews with the supervisor or Assistant supervisor. In addition, the Press officer leads a flexible information team which provides assistance for information activities and



Information team.

is involved in promotional events (in particular the organisation of 'Data Protection Day' and the 'EU Open Day', see Section 5.9).

### Media contacts

The EDPS aims to be as accessible as possible for journalists in order to allow the public to follow his work. He regularly informs the media mainly through press releases, interviews, background discussions, and press conferences. The handling of media enquiries (requests for information or comments), which are received on a recurrent basis — mainly as regards issues of interest for the public at large — allows for additional contact with the media.

In 2008, the press service issued 13 press releases, or an average of one per month throughout the year. Most of them related to new legislative opinions which were of high public general relevance. Among the issues covered were the EU's proposed external border management system, biometrics in passports, the review of the e-privacy directive, public access to EU documents, transatlantic information sharing for enforcement purposes, and the adoption of the framework decision on data protection in the third pillar. Press releases are published on the EDPS's website and on the European Commission's inter-institutional database of press releases (RAPID) in English and French. They are distributed to a regularly updated network of journalists and interested parties. The information provided in the press releases usually results in significant media coverage, as they are often taken up 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 information technology companies.

In 2008, the EDPS gave about 25 interviews to journalists from the print, broadcast and electronic media throughout Europe and in third countries. This resulted in a number of quotes and articles in the national press (e.g. *Daily Telegraph*, *BBC*, *New York Times*, various newspapers from the German and Dutch press, Hungarian News Agency), the international and EU press (e.g. *The Economist*, *European Voice*, *Euractiv*), publications and websites specialised in data protection and



Peter Hustinx and Joaquín Bayo Delgado presenting their 2007 Annual Report to the press.

information technology issues, as well as interviews on radio and television (e.g. Deutsche Welle, Dutch Television, Radio 1 RAI, Polish radio). The interviews covered issues such as EU passenger names records (PNR), the data retention directive, the proposed EU border management system, the American visa waiver programme, the Schengen information system (SIS), privacy in healthcare and data protection adequacy at the EU level.

### 5.5. Requests for information

The number of public enquiries for information or assistance rose to more than 180 in 2008 (compared to 160 requests in 2007). These requests come from a wide range of individuals and actors, ranging from stakeholders operating in the EU environment and/or working in the field of privacy/data protection and information technology (law firms, consultancies, lobbyists, ONGs, 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. These requests are primarily received via the general e-mail account of the EDPS and, more occasionally, by regular mail.

‘Requests for information’ correspond to a broad category of enquiries which comprises, *inter alia*, general questions on data protection policies and legislation both in the EU and at national level, but also more specific and technical questions on a given aspect linked to privacy and the protection of personal data. By way of examples, requests for information were received in 2008 concerning security incidents related to data breaches, biometric technology, RFID, privacy on the Internet — including social networking, e-monitoring and call recording, processing of images, launch of Google Street View, review of the EU telecoms package, transfer of personal data to third countries, as well as provisions of the Lisbon Treaty on the protection of personal data.

It is worth pointing out that a significant number of requests for information received from the general public deal with national issues for which the

EDPS has no competence. In such cases, a reply is sent specifying the mandate of the EDPS and advising that the recipient refer to the relevant authority, usually the national data protection authority of the concerned Member State.

Requests that go beyond the purely informative aspect and which, therefore, require a more in-depth analysis are usually dealt with by case officers. In 2008, they covered issues such as PNR data, SIS, data protection in a transatlantic perspective, biometrics in Eurodac, data protection in criminal proceedings, binding corporate rules and the interface between data protection and competition law.

As in previous years, most of the requests were received in English and, to a lesser extent, in French, German, Italian and Spanish. This allowed for fast replies from the press service, well within the limit of 15 working days. Only a few requests were received in other EU official languages, which required the assistance of the Council's translation service.

## 5.6. Study visits

As part of the efforts aimed at further increasing his visibility, as well as interaction with the academic world, the EDPS welcomes visits from student groups specialised in the field of European law, data protection and/or IT security issues. In March 2008, the EDPS for instance welcomed a group of international and European law students from the University of Tilburg.

Other groups of visitors were also welcomed in the EDPS's premise, including a delegation from the Committee on Justice of the Dutch House of Representatives in May 2008. The IT-Political Association of Denmark also visited the EDPS in February to discuss the implications of recent data retention and surveillance initiatives on privacy and data protection.

## 5.7. Online information tools

### Website

The website remains the most important communication and information tool of the EDPS.

It is also the medium through which visitors can access all the various documents produced within the framework of the EDPS's activities (opinions on prior-checks and proposals for EU legislation, comments, work priorities, publications, speeches, press releases, newsletters, events' information, etc.). The website is therefore updated nearly on a daily basis with the upload of relevant documents and information.

### *Content developments*

As announced in the 2007 annual report, information tools were developed in 2008 with a view to further improving the content provided by the website and to better meet visitors' expectations.

Such improvements included the development of a Glossary of terms related to the protection of personal data. The glossary consists of 75 terms which provide links to external and internal pages of the EDPS's website for complementary information. It is primarily designed to provide visitors of the website with a tool that can help to achieve a better understanding of the activities and work of the EDPS, as well as of data protection issues in a more general context. In parallel, a 'Questions and answers' section was also developed. The purpose was notably to clarify the mandate, the competence and fields of action of the EDPS, and to provide an instant guide to most common queries. The section provides background information and, where relevant, practical guidelines, on issues such as the duties and competences of the EDPS, data protection legislation at EU level, the data subject's rights, rules governing the processing of personal data and the transfer of personal data.

Publication of these two new sections on the website is scheduled for the beginning of 2009. As a complement to the 'Questions and answers' section, a document on most 'Frequently asked questions' is also in the pipeline in order to provide targeted answers to different profiles and concerned audiences (e.g. EC staff, visitors, applicants to vacant posts in Community institutions and bodies).

### *Technical developments*

To enhance the performance of the EDPS's website, launched in 2007, technical improvements

were brought about in 2008 with a view to facilitate the navigation. This was the case for pages containing a high number of documents, in particular the page listing the EDPS's prior-check opinions, which had to be reorganised and split in order to guarantee the smooth running of the website.

In addition to the improvement of the website's general performance, an 'advanced search' functionality was added to the site. This new functionality allows visitors to combine search terms and make specific searches in PDF documents. The advanced search will however need to be fine-tuned in 2009 to achieve better and more reliable results.

A statistical tool providing traffic and navigation data was installed in January 2008. Statistical information shows that from 1 February to 31 December 2008 the website received a total of 81 841 unique visitors, with a peak of 10 095 visitors in May at the time of the presentation of the 2007 annual report. In addition to the homepage and the 'advanced search', pages related to the 'News', press releases, and annual reports were among the most consulted pages of the site.

In the framework of the inter-institutional Internet Editorial Committee (CEiii), the EDPS's webmaster continued to take part in discussions on the development of an EU inter-institutional search tool that should later become available on the Europa website.

In 2009, the website will be updated to reflect the appointment of the Supervisor and the Assistant Supervisor for the second mandate. Technical developments, in particular as regards the advanced search functionality, as well as improvements in the design are also in preparation. In addition, a study will be launched as to a possible overhaul of the homepage with a view to making it more dynamic by giving more prominence to latest news on the EDPS's activities.

### **Newsletter**

The EDPS newsletter remains an efficient tool to raise awareness of EDPS's latest activities, and to draw attention to recent additions to the website. It

provides news related to the latest EDPS's opinions on EU legislative proposals and on prior checks, and includes information about forthcoming events/conferences in the field and recent speeches from the EDPS. The newsletters are available on the EDPS's website and an automatic subscription feature is also offered on the relevant page.

Five issues of the EDPS newsletter were published in 2008, 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 635 people at the end of 2007 to a total of 880 at the end of 2008. 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 has led to the need to provide an upgraded publication that would include a more user-friendly design and layout. The aim is also to provide a revised architecture for the newsletter to improve readability.

To that end, preparatory work was undertaken in 2008 with a communication agency specialised in publishing information on European policies in order to identify the needs and to consider how to proceed. Work will continue in 2009 in order to bring the project to fruition.

## **5.8. Publications**

### **Annual report**

The annual report is the EDPS's key publication. Published as a rule every spring, it provides an overview of the EDPS's activities in the main operational fields of supervision, consultation and cooperation during the reporting year. It also describes what has been achieved in terms of external communication as well as developments in administration, budget and staff.

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

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

The Supervisor presented the EDPS's annual report 2007 to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs on 26 March 2008.

A press conference was then organised in mid-May to present the report to the media. The press conference highlighted the impact of the Lisbon Treaty in terms of enhanced protection of personal data. The EDPS took this opportunity to emphasise that the new Treaty should be seen as an opportunity for the EU administration to demonstrate that effective protection of personal data is a basic value underlying EU policies.

### Information brochure

With the aim of raising awareness of the new institution, two different brochures on the EDPS were developed in the wake of its setting up at the end of 2004. One presents the EDPS from an institutional point of view, while the other one describes the rights of the data subjects whose data are processed by Community institutions and bodies.

The development of an updated information brochure merging the two current ones was initiated in 2008, especially in view of the first EDPS mandate coming to an end in January 2009. This necessary update will also provide the opportunity to produce a modernised brochure. This new information material will highlight key points about the EDPS and the protection of personal data at EU level, as well as practical information, in a dynamic and straight-to-the-point editorial style.

## 5.9. Awareness-raising events

Participating in EU-related events offers an excellent opportunity for the EDPS to raise awareness about the rights of the data subjects and the

obligations of the Community institutions and bodies in relation to privacy and the protection of personal data.

### Data Protection Day

The Member States of the Council of Europe and the European institutions celebrated Data Protection Day for the second time on 28 January 2008. This date marks the anniversary of the Council of Europe's Convention 108, the first legally binding international instrument related to data protection, adopted in 1981.

The event gave the EDPS the opportunity to focus on raising awareness among EU staff and any interested person about their rights and obligations regarding data protection. For that purpose, an information stand was set up on three consecutive days in the European Parliament, the European Commission, and the Council premises. The EDPS outlined his supervisory, consultative and cooperative roles, as well as his achievements and current activities. The EDPS's stand was set up in cooperation with the data protection officers of the relevant institutions, who presented their activities as well.

Overall, the EDPS staff welcomed about 250 visitors. Various information materials presenting the EDPS's work were distributed, together with a range of promotional items. Visitors also had



EDPS stand in the European Commission on the occasion of Data Protection Day (Brussels, 30 January 2008).

the opportunity to test their knowledge of data protection issues in a short quiz and to take part in a prize draw.

For the next edition of Data Protection Day, the aim will be to further develop this particular activity, especially through enhanced cooperation with the network of data protection officers and the provision of a wider range of information materials.

### EU Open Days

On 7 June 2008, the EDPS's office also participated, as it does now each year, in the Open Days at the European institutions organised in the European Parliament in Brussels.

The EDPS had a stand located in the European Parliament's main building and staff members were present to answer questions from visitors on the EDPS's role and activities.

Various information materials presenting the EDPS's work were distributed to visitors, together with a range of promotional items (pens, stickers, mugs and USB keys displaying the EDPS logo). A quiz on the EDPS's role and data protection at Community level was also made available on the spot and offered the opportunity to participate in a prize draw.



EDPS stand in the European Parliament during the EU Open Day (Brussels, 7 June 2008).

## 5.10. Priorities for 2009

In 2009, the EDPS's information and communication activities will concentrate on the following priorities:

- **to further develop the website:** in addition to the publication of new content, technical and graphic improvements will be brought to the website in order to facilitate the navigation, to make the content visually more attractive and to provide more visibility and immediate access to the 'News'; relevant parts of the website will also need to be updated following the appointment of the EDPS and Assistant EDPS for the next mandate (2009–14);
- **to finalise the newsletter upgrade** with the aim of offering readers a modern, reader-friendly information tool;
- **to finalise the new information brochure** on the EDPS and the protection of personal data in Community institutions and bodies;
- **to further clarify the EDPS's competence:** among the citizens who have heard about the EDPS, a sizeable number of them are not well aware of its competence and tend to see it as a kind of European umbrella data protection body to which one can refer when encountering problems at national level; this misunderstanding needs to be properly addressed; a first step will be to better clarify the role of the EDPS in the new information brochure and on the website, in particular through the 'Questions and answers' section.
- **to streamline the EDPS's press policy,** in particular as regards the publication of press releases and the handling of requests for information, interviews, comments, etc. from the media; internal guidelines relating to the publication of press releases will be drafted; the EDPS's practice to handle press requests will also be clarified to make explicit how and through which channel(s) they should be made.



## 6. Administration, budget and staff

### 6.1. Introduction

With the aim of further consolidating its positive start and, consequently, handling new tasks assigned, additional resources both in terms of budget (increasing from EUR 4 955 726 in 2007 to EUR 5 307 753 in 2008) and staff (from 29 to 33) have been attributed to the EDPS.

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>(68)</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.

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



Personnel, Budget and Administration Unit.

<sup>(68)</sup> A list of administrative agreements and decisions is available in Annex I.

### 6.2. Budget

The budget adopted by the budgetary authority for 2008 amounted to EUR 5 307 753. This represents a 7.1 % increase compared with the budget for 2007.

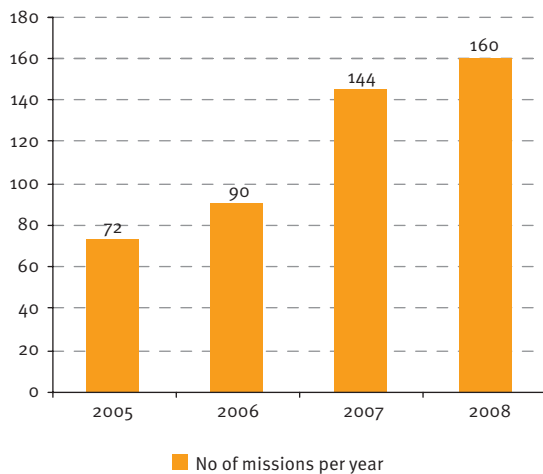
In 2008, a new budget terminology was applied. It is based on the previous years of experience of the EDPS, taking into account the specific needs of the institution and ensuring the transparency required by the budgetary authority.

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. An important improvement of the structuring and filing of financial documents has been achieved with the adoption of a new decision which takes into account the increasing quantity of financial files. The use of the new budget terminology guarantees ongoing transparency and easy handling.

Several internal handling processes have been optimised to keep the institution attuned to the steadily increasing number of financial files.

**Assistance from the Commission** continued to be provided, particularly regarding the accounts, since the Accounting Officer of the Commission is also appointed as the Accounting Officer of the EDPS.

In its report on the 2007 financial year, the European Court of Auditors stated that the audit had not given rise to any observations.



Evolution of number of missions

An important part of the budget is dedicated to translations. The EDPS's opinions on legislative proposals are translated into 23 European official languages. These opinions are published in the Official Journal of the European Union. Since 2005, the number of opinions has increased steadily, as well as the number of other documents to be translated. Opinions on prior checks and other published documents are usually translated into the EDPS's working languages only.

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 EDPS manages the financial aspects of the missions with assistance of the Paymaster's Office (PMO).

### 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 33 staff).

#### 6.3.1. Recruitment

The growing visibility of the institution is leading to an increased workload, together with an expansion of tasks. The significant growth of workload in 2008 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 four posts in 2008 (three administrators and one assistant). This request was authorised by the budgetary authority, with the number of staff increasing from 29 in 2007 to 33 in 2008. Vacancy notices were published at the beginning of 2008 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 PMO and the medical service.

The EDPS has access to the services provided by the European Personnel Selection Office (EPSO) and participates in the work of its management board, presently as an observer.

#### 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. 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 Traineeship Office of the Commission's Directorate-General for Education and Culture, which has continued to provide valuable support thanks to the extensive experience of its staff. In September 2008, a new service level agreement was signed, improving a number of administrative practices, namely the payment of grants and other financial issues.

### 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>(69)</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 benefits of this programme work 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 and invited to assist in seeking suitable candidates. The Commission's Directorate-General for Personnel and Administration provides valuable administrative assistance for the organisation of the programme.

In 2008, two national experts were seconded, one from the Spanish DPA and another from the Greek DPA, replacing the former British and Hungarian national experts.

<sup>(69)</sup> EDPS's decision of 10 November 2005.

### 6.3.4. Organisation chart

The EDPS's 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 25 members of staff who are in charge of the operational aspects of data protection tasks. They work under the direct authority of the Supervisor and the Assistant Supervisor in two main fields dealing with supervision and consultation. The increasing workload has prompted the creation of a new function as coordinator. To this end, eight coordinators have been designated in the consultation and supervision teams, while the press officer is coordinating a small information team.

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

### 6.3.5. Social dialogue

In accordance with Article 9 of the Staff Regulations of Officials of the European Communities, the Supervisor adopted on 8 February 2006 a decision setting up a staff committee. The Committee is consulted on a range of general implementing provisions for the Staff Regulations and on other internal rules adopted by the institution. In 2008, the staff committee organised social activities for the staff outside the office.

### 6.3.6. Training

In 2008, the process of expanding and improving the EDPS staff's knowledge, competencies and attitudes, so that each staff member can optimally contribute to the achievement of the institution's objectives, has continued. According to the internal training decision, a training plan was established, based on the staff needs identified through a survey conducted among the staff.

The main learning areas identified in the general orientations, annexed to the internal training decision, became a priority in 2008. These included mandatory trainings for newcomers, compulsory training for specific functions and language training courses.

In line with the objective to develop an excellence in the field of data protection, EDPS staff were allowed

to participate in professional external trainings in the field of information security. The participation at seminars and information sessions in the area of data protection was also encouraged.

To enable newcomers to become self-reliant and develop personally and professionally, a mentoring programme was implemented in addition to the information day already in place.

EDPS staff benefit from training courses organised by other European institutions (namely the European Commission and the European Parliament) and by interinstitutional bodies (the European Administrative School — EAS).

The EDPS continued to participate in interinstitutional committees (EAS' interinstitutional working party, interinstitutional committee for language training, etc.) with the aim to share a common approach in a sector where the needs are essentially similar across the institutions and allow for economies of scale.

In 2008, the EDPS signed, together with the other institutions, a new protocol on the harmonisation of the cost of the interinstitutional language courses.

### **6.3.7. Social activities**

An information day has been structured for newly-recruited colleagues. During the welcome day, all newcomers are personally welcomed by the Supervisor and the Assistant Supervisor. In addition to their mentor, they also meet with the members of the administrative unit who give them information on the specificities of the institution and provide them with the EDPS administrative guide. The EDPS is working on a cooperation agreement with the Commission to help the integration and installation of new colleagues, for instance by providing legal assistance in private matters (rental contracts, buying a house, etc.).

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

The EDPS continued to develop inter-institutional cooperation in the field of social facilities:

the children of the EDPS staff have access to the *crèches*, the after-school childcare and the outdoor childcare centres of the Commission, as well as to the European schools. They have also the opportunity to participate in the European Parliament's St Nicholas' party.

### **6.3.8. Protocol on the privileges and immunities of the European Communities.**

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.

## **6.4. Control functions**

### **6.4.1. Internal control**

#### **Risk assessment and implementation of internal control**

The assessment of risks related to the EDPS's activities is still at an early stage. 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.

In the meantime, the EDPS has adopted specific internal control procedures deemed to be best suited to its needs, 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.

#### **Internal evaluation of the internal control environment**

The evaluation performed by the EDPS's services has demonstrated the functionality and efficiency of the internal control system, and identified some recommendations for improvements in the future. The implementation of these recommendations was a priority in 2008. The internal report on internal controls showed a high rate of implementation of internal recommendations (80 %).

### **Annual activity report and declaration of assurance**

The EDPS took note of the annual activity report and the included declaration of assurance signed by the Authorising Officer by delegation. 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 see to it that the Authorising Officer by delegation continues her efforts to ensure that the reasonable assurance provided by the declaration included in her annual activity report is effectively supported by appropriate internal control systems.

#### **6.4.2. Internal audit**

The 2004 administrative cooperation agreement, prolonged in 2006, nominated the Commission's internal auditor as the auditor of the EDPS. On this basis, the first audit visit took place in 2006 and the first audit report made by the Internal Audit Service (IAS) was received in September 2007. The report confirmed the capacity of the EDPS's 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 be put in place progressively, along with the evolution of the tasks that are entrusted to the EDPS.

The implementation of IAS recommendations agreed by the EDPS has been undertaken on the basis of an action plan drawn up in early 2008.

In December 2008, the IAS performed a follow-up audit. The report on this audit has not been received yet.

#### **6.4.3. Security**

Aware of the degree of confidentiality required for some areas of his activities, the EDPS adopted a decision in 2008 on the security measures applicable in the institution. The decision lays down the basic principles and minimum standards of security to be respected in an appropriate manner by all staff. This comprehensive decision includes

measures on management of confidentiality of information, informatics security, as well as on safety conditions of persons and premises.

#### **6.4.4. Data Protection Officer**

The process to identify processing operations containing personal data and to determine which operations are subject to prior checking has continued in 2008. An inventory of internal operations has been finalised. The inventory, as a practical tool, aims to steer the notification process. On account of his specific position, the EDPS has developed a simplified notification system for cases subject to prior checking.

On this basis, the first notification process was launched during 2008. Moreover, different privacy statements (staff notes) have been drafted providing the information contained in Articles 11 and 12 of Regulation (EC) No 45/2001.

In order to allow data subjects to exercise their rights, a specific mailbox has been created to that effect.

The participation in the DPO network meetings permitted the sharing of common experiences and discussion on horizontal issues.

### **6.5. Infrastructure**

On the basis of the administrative cooperation agreement, the EDPS is located in the premises of the European Parliament, which furthermore assists the EDPS mainly in the fields of information technology (IT) and telephone infrastructure. The EDPS accommodated all new staff by restructuring the workspace. The resultant optimised use of the allocated space reached its full capacity in 2008.

The EDPS has independently continued to manage his furniture and IT goods inventory, with the assistance of the European Parliament's services.

### **6.6. Administrative environment**

#### **6.6.1. Administrative assistance and inter-institutional cooperation**

The EDPS benefits from the inter-institutional cooperation in many areas of administration by

virtue of the administrative cooperation agreement concluded in 2004 and extended in 2006 for a three-year period, with the Secretaries-General of the Commission, the Parliament and the Council. This cooperation is of considerable added value to the EDPS in terms of increased efficiency and economies of scale. It also 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, the inter-institutional cooperation continued in 2008 with various Commission directorates-general (Personnel and Administration; Budget; Internal Audit Service; Education and Culture), the Paymaster's Office, various European Parliament services (information and technology services, particularly with arrangements for the new version of the EDPS's website; fitting out of the premises, building security, printing, mail, telephone, supplies, etc.) and with the Council (regarding translation work).

Service-level agreements that have been signed since the beginning with the various institutions and their departments are regularly updated. In September 2008, the EDPS signed a new service-level agreement with the medical service of the Commission.

Additionally, the EDPS signed a delegation to PMO of day-to-day activities related to the management of pension rights. Agreements covering new areas are in preparation.

Direct access from EDPS's premises to some of the Commission's financial management applications has been obtained with a view to facilitate cooperation between Commission departments and the EDPS, and to improve the exchange of information between the services.

The new version of the EDPS's website, developed in cooperation with the relevant services of the European Parliament, was completed in 2008. Nevertheless, some problems related to the specific software that had been selected for its development have slowed down the launch of further web functionalities already developed. The EDPS expects to complete this project in the course of 2009.

Participation in the interinstitutional call for tenders for general and language training courses, insurance, and furniture continued in 2008, allowing the institution to increase its efficiency in many administrative areas and to progress towards greater autonomy. Regarding office supplies, the EDPS participated in the European Parliament's call for tender.

The EDPS continued to participate in various interinstitutional committees. This participation is particularly active in *Comité de Gestion Assurances maladies* (CGAM), *Comité de Préparation pour les Questions Statutaires* (CPQS) and *Comité du Statut*, where the EDPS is represented in various working groups. However, because of the limited size of the institution, such participation had to be limited to only a few committees. This participation contributed to increase the visibility of the EDPS in the other institutions and encouraged the continuous exchange of information and good practice.

### 6.6.2. 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's office. On the occasion of the welcome day, newly recruited colleagues are provided with an 'administrative guide', which contains all the EDPS's internal rules and informs them about the specificities of the institution. The document is regularly updated.

Five important internal decisions were adopted in 2008:

- Rules of 16 June 2008 on the reimbursement of expenses incurred by persons from outside the EDPS's services invited to attend meetings in an expert capacity;
- Decision of 8 August 2008 of the authorising officer by delegation, related to the archiving of financial and supporting documents;

- Decision of 2 October 2008 of the Supervisor regarding general implementing rules of Article 45a of the Staff Regulations (certification);
- Decision of 16 December 2008 of the Supervisor adopting security measures within the EDPS;
- Decision of 19 December 2008 of the Supervisor on the appointment of a local security officer for the EDPS.

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, existing rules will be subject to an evaluation, to be carried out two years after their adoption, and may therefore be amended accordingly.

### 6.6.3. Document management

The implementation of a new electronic mail management system (GEDA) has been going on, despite some delays due to unexpected difficulties; it should be finalised in 2009, with the support of the European Parliament's services. This implementation is seen as a first step in the development of a case flow management system for improved support to EDPS's activities.

## 6.7. Objectives for 2009

The objectives set for 2008 were fully achieved. In 2009, the EDPS will continue the consolidation process undertaken previously and further develop some activities.

The EDPS will carry on with the adoption of new internal financial rules adapted to its size. As to financial software, the EDPS will continue the 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. The EDPS intends to sign a cooperation agreement with the Commission (Adminfo) to help the integration and installation of new colleagues. In parallel, the EDPS will continue to develop the office's administrative environment and to adopt general implementing provisions for the Staff Regulations.

The EDPS intends to launch a general competition in data protection, organised with the European Personnel Selection Office (EPSO), in order to recruit highly specialised staff.

Concerning human resources management software (mainly missions: MIP's; 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 EDPS plans to perform a thorough risk assessment, in order to evaluate whether the existing internal control standards are adequate in view of the current practices of the institution.

The implementation of the improvements identified during the assessment of the internal control system, as well as the implementation of the recommendations of the internal audit service, will continue to be an important priority.

The DPO will continue to ensure the internal application of the provisions of Regulation (EC) No 45/2001. A register of notifications will be set up.

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 2009.

The EDPS intends to finalise, with the help of the European Parliament, the implementation of the electronic mail management system 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 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 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 more than 40 Member States of the Council of Europe, including all EU Member States.

Directive 95/46/EC was based on the principles of Convention 108, but specified and developed them in many ways. It aimed to provide a high level of protection and a free flow of personal data in the EU. When the Commission made the proposal for this directive in the early 1990s, it stated that Community institutions and bodies should be covered by similar legal safeguards, thus enabling them to take part in a free flow of personal data, subject to equivalent rules of protection. However, until the adoption of Article 286 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 bodies

and on the free movement of such data, which entered into force in 2001 <sup>(70)</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 and subject to ratification by all Member States, 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 horizontal subject 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.

### 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>(70)</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 Data Protection Officer (DPO). These officers have the task of ensuring the internal application of the provisions of the regulation, including the proper notification of processing operations, in an independent manner. All Community institutions and most bodies now have these officers, and some of them have been active for several years. This means that important work has been done to implement the regulation, even in the absence of a supervisory body. These officers may also be in a better position to advise or to intervene at an early stage and to help to develop good practice. Since the DPO has the formal duty to cooperate with the EDPS, this is a very important and highly appreciated network to work with and to develop further (see Section 2.2).

### Tasks and powers of 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 and intervening in cases before the Court of Justice are also important tasks. These consultative activities of the EDPS are more widely discussed in chapter 3 of this report.

The duty to cooperate with national supervisory authorities and supervisory bodies in the ‘third pillar’ has a similar impact. As a member of the Article 29 Data Protection Working Party, established to advise the European Commission and to develop harmonised policies, the EDPS has the opportunity to contribute at that level. Cooperation with supervisory bodies in the ‘third pillar’ allows him to observe developments in that context and to contribute to a more coherent and consistent framework for the protection of personal data, regardless of the ‘pillar’ or the specific context involved. This cooperation is further dealt with in chapter 4 of this report.

## Annex B

## Extract from Regulation (EC) No 45/2001

**Article 41 — European Data Protection Supervisor**

1. An independent supervisory authority is hereby established referred to as the European Data Protection Supervisor.
2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies.

The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47.

**Article 46 — Duties**

The European Data Protection Supervisor shall:

- (a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;
- (b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;
- (c) monitor and ensure the application of the provisions of this regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;
- (d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of

fundamental rights and freedoms with regard to the processing of personal data;

- (e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
- (f) cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body;
 

also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;
- (g) participate in the activities of the working party on the protection of individuals with regard to the processing of personal data set up by Article 29 of Directive 95/46/EC;
- (h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);
- (i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the data protection officers under Article 26;
- (j) carry out a prior check of processing notified to him or her;
- (k) establish his or her rules of procedure.

**Article 47 — Powers**

1. The European Data Protection Supervisor may:
  - (a) give advice to data subjects in the exercise of their rights;
  - (b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where

- appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;
- (c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;
  - (d) warn or admonish the controller;
  - (e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;
  - (f) impose a temporary or definitive ban on processing;
  - (g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;
  - (h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;
  - (i) intervene in actions brought before the Court of Justice of the European Communities.
2. The European Data Protection Supervisor shall have the power:
- (a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;
  - (b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this regulation is being carried out there.

## Annex C

## List of abbreviations

ARES	Advanced Records System
CCL	Common Conservation List
CCTV	Closed circuit television
CdT	Translation Centre for the Bodies of the European Union
Cedefop	European Centre for the Development of Vocational Training
CFCA	Community Fisheries Control Agency
CIS	Custom Information System
CoA	Court of Auditors
CoR	Committee of the Regions
CPCS	Consumer Protection Cooperation System
CPVO	Community Plant Variety Office
CRS	Computerised Reservation System
DG JLS	Directorate-General for Justice, Freedom and Security
DG ADMIN	Directorate-General for Personnel and Administration
DG EAC	Directorate-General for Education and Culture
DG EMPL	Directorate-General for Employment, Social Affairs and Equal Opportunities
DG INFSO	Directorate-General for the Information Society and Media
DIGIT	Directorate General Informatics
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
ECJ	European Court of Justice
ECRIS	European Criminal Records Information System
EESC	European Economic and Social Committee
EFSA	European Food Safety Authority
EIB	European Investment Bank
EMPL	Committee on Employment and Social Affairs in European Parliament
ENISA	European Network and Information Security Agency
ECHR	European Convention on Human Rights
EMA	European Medicines Agency
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMSA	European Maritime Safety Agency
EPSO	European Personnel Selection Office
ETF	European Training Foundation

EU	European Union
EUMC	European Monitoring Centre on Racism and Xenophobia
Eurofound	European Foundation for the Improvement of Living and Working Conditions
EWS	Early Warning System
FIDE	Customs Files Identification Database
FP7	Seventh research framework programme
FRA	European Union Agency for Fundamental Rights
IAS	Internal Auditing Service
IGC	Inter-Governmental Conference
IMI	Internal Market Information System
IMS	Identity Management Service
JRC	Joint Research Centre
JSB	Joint Supervisory Body
LIBE	Committee on Civil Liberties, Justice and Home Affairs in European Parliament
MoU	Memorandum of Understanding
NSA	National Security Authority
OECD	Organisation for Economic Cooperation and Development
OHC	Occupation Health Centre
OHIM	Office for Harmonisation in the Internal Market
OLAF	European Anti-fraud Office
PEP	Politically Exposed Person
PMO	European Commission Paymaster's Office
PNR	Passenger Name Record
R & D	Research and development
RFID	Radio Frequency Identification
SIS	Schengen Information System
SWIFT	Society for Worldwide Interbank Financial Telecommunication
Third pillar	Police and judicial cooperation in criminal matters
TIM	Time management system
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)

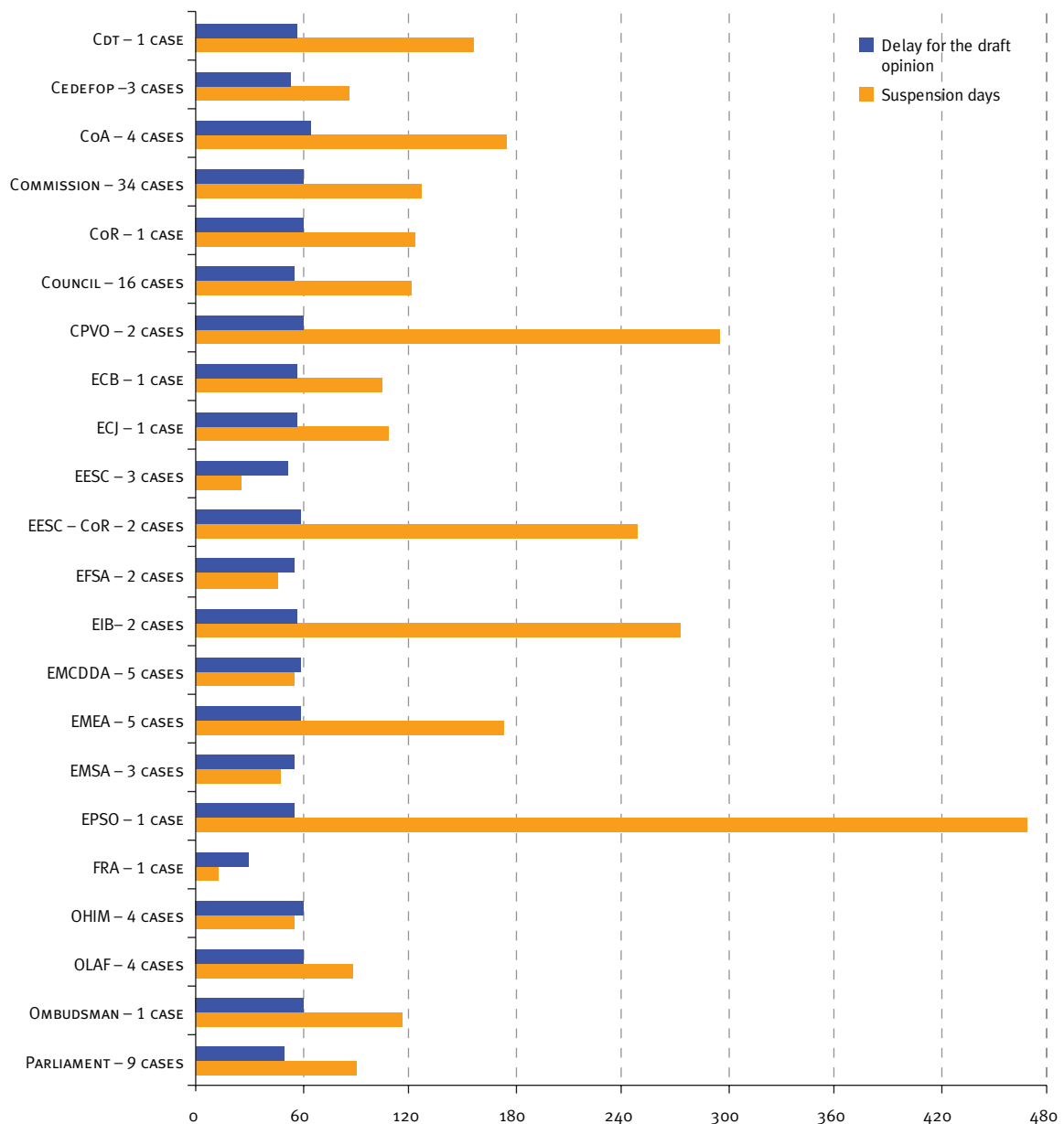
Organisation	Name	E-mail
European Parliament	Jonathan STEELE	dg5data-protection@europarl.europa.eu
Council of the European Union	Pierre VERNHES	data.protection@consilium.europa.eu
European Commission	Philippe RENAUDIÈRE	data-protection-officer@ec.europa.eu
Court of Justice of the European Communities	Marc SCHAUSS	dataprotectionofficer@curia.europa.eu
Court of Auditors	Jan KILB	data-protection@eca.europa.eu
European Economic and Social Committee	Maria ARSENE	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 Ombudsman	Loïc JULIEN	dpo-euro-ombudsman@ombudsman.europa.eu
European Data Protection Supervisor	Giuseppina LAURITANO	giuseppina.lauritano@edps.europa.eu
European Central Bank	Martin BENISCH	DPO@ecb.int
European Anti-Fraud Office (OLAF)	Laraine LAUDATI	laraine.laudati@ec.europa.eu
Translation Centre for the Bodies of the European Union	Benoît VITALE	data-protection@cdt.europa.eu
Office for Harmonization in the Internal Market (OHIM)	Ignacio DE MEDRANO CABALLERO	dataprotectionofficer@oami.europa.eu
European Union Fundamental Rights Agency (FRA)	Nikolaos FIKATAS	nikolaos.fikatas@fra.europa.eu
European Medicines Agency (EMA)	Vincenzo SALVATORE	data.protection@emea.europa.eu
Community Plant Variety Office (CPVO)	Véronique DOREAU	doreau@cpvo.europa.eu
European Training Foundation (ETF)	Liia KAARLOP	liia.kaarlop@etf.europa.eu
European Network and Information Security Agency (ENISA)	Andreas MITRAKAS	dataprotection@enisa.europa.eu
European Foundation for the Improvement of Living and Working Conditions (Eurofound)	Markus GRIMMEISEN	mgr@eurofound.europa.eu
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	Cécile MARTEL	cecile.martel@emcdda.europa.eu
European Food Safety Authority (EFSA)	Claus REUNIS	dataprotectionofficer@efsa.europa.eu
European Maritime Safety Agency (EMSA)	Malgorzata NESTEROWICZ	malgorzata.nesterowicz@emsa.europa.eu
European Agency for Reconstruction (EAR)	Richard LUNDGREN	richard.lundgren@ear.europa.eu
European Centre for the Development of Vocational Training (Cedefop)	Spyros ANTONIOU	spyros.antoniou@cedefop.europa.eu
Education, Audiovisual and Culture Executive Agency (EACEA)	Hubert MONET	hubert.monet@ec.europa.eu
European Agency for Safety and Health at Work (OSHA)	Terry TAYLOR	taylor@osha.europa.eu
Community Fisheries Control Agency (CFCA)	Rieke ARNDT	rieke.arndt@cfca.europa.eu
European GNSS Supervisory Authority	Christina TSALI	christina.tsali@gsa.europa.eu
European Railway Agency (ERA)	Zographia PYLORIDOU	zographia.pyloridou@era.europa.eu

Organisation	Name	E-mail
Public Health Executive Agency (PHEA)	Eva LÄTTI	eva.latti@ec.europa.eu
European Centre for Disease Prevention and Control (ECDC)	Elisabeth ROBINO	elisabeth.robino@ecdc.europa.eu
European Environment Agency (EAA)	Gordon McINNES	gordon.mcinnnes@eea.europa.eu
European Investment Fund (EIF)	Jobst NEUSS	j.neuss@eif.org
European Agency for the Management of Operational Cooperation at the External Border (Frontex)	Sakari VUORENSOLA	sakari.vuorensola@frontex.europa.eu
European Aviation Safety Agency (EASA)	Arthur BECKAND	arthur.beckand@easa.europa.eu
Executive Agency for Competitiveness and Innovation (eaci)	Elena FIERRO SEDANO	elena.ferro-sedano@ec.europa.eu
Trans-European Transport Network Executive Agency (TEN-T EA)	Elisa Dalle Molle	Elisa.dalle-molle@ext.ec.europa.eu
European Chemicals Agency (ECHA)	Minna HEIKKILA	minna.heikkila@echa.europa.eu



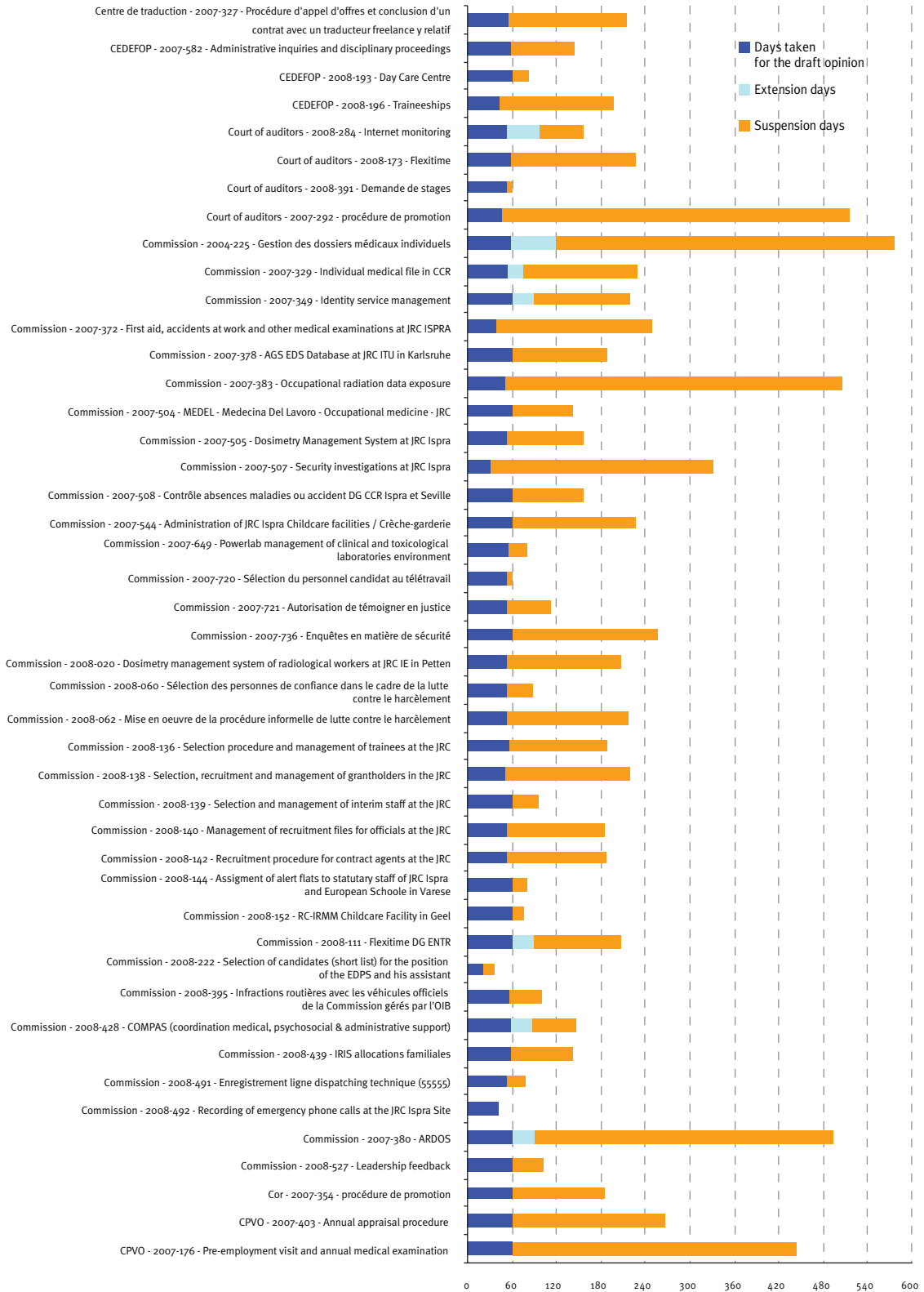
## Annex E

## Prior checking handling time per case and per institution

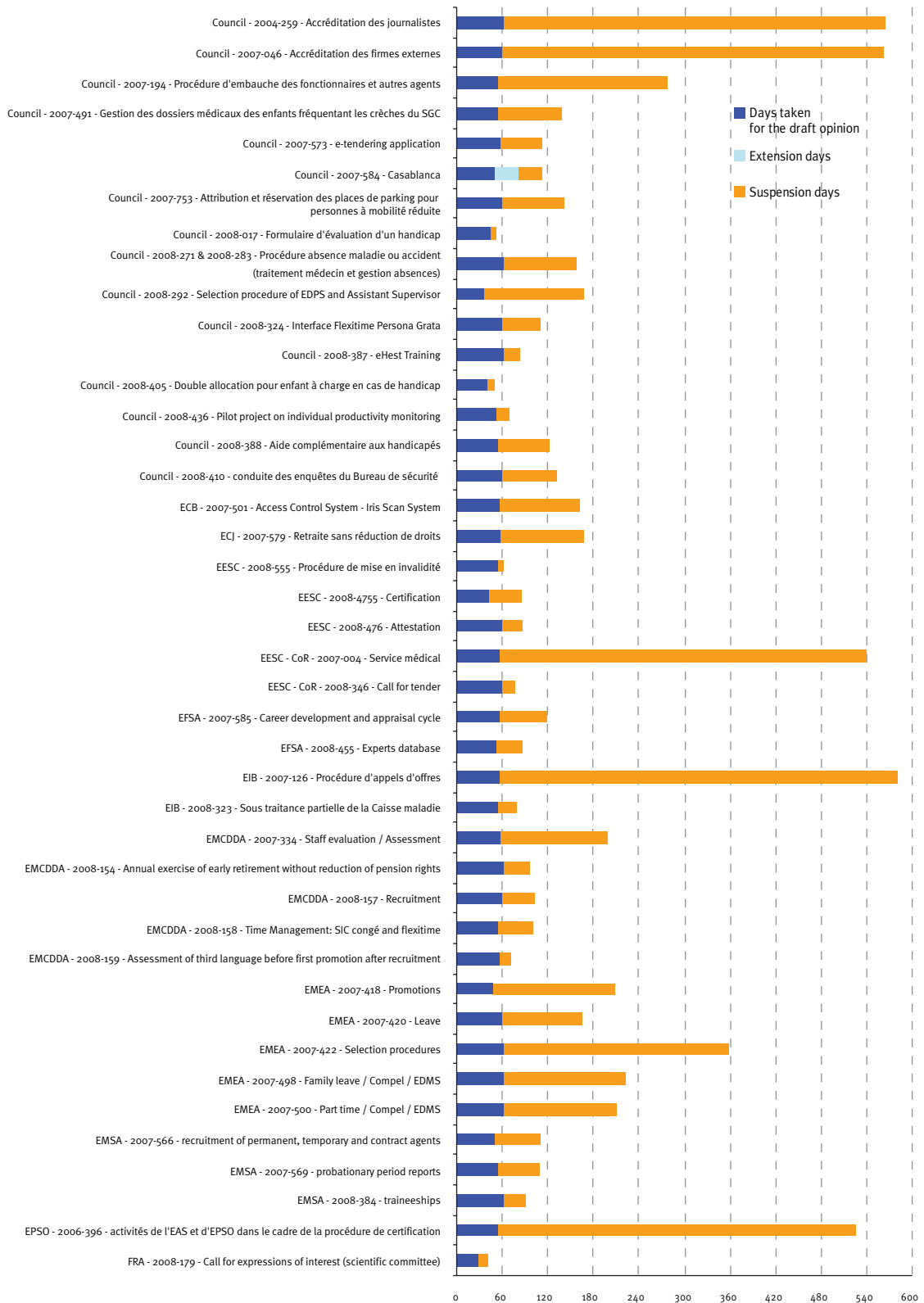


NB: Delays for the draft opinions do not include the month of August in ex-post cases received before 1/09/08. Suspension days include the suspension for comments on the draft, normally 7 to 10 days.

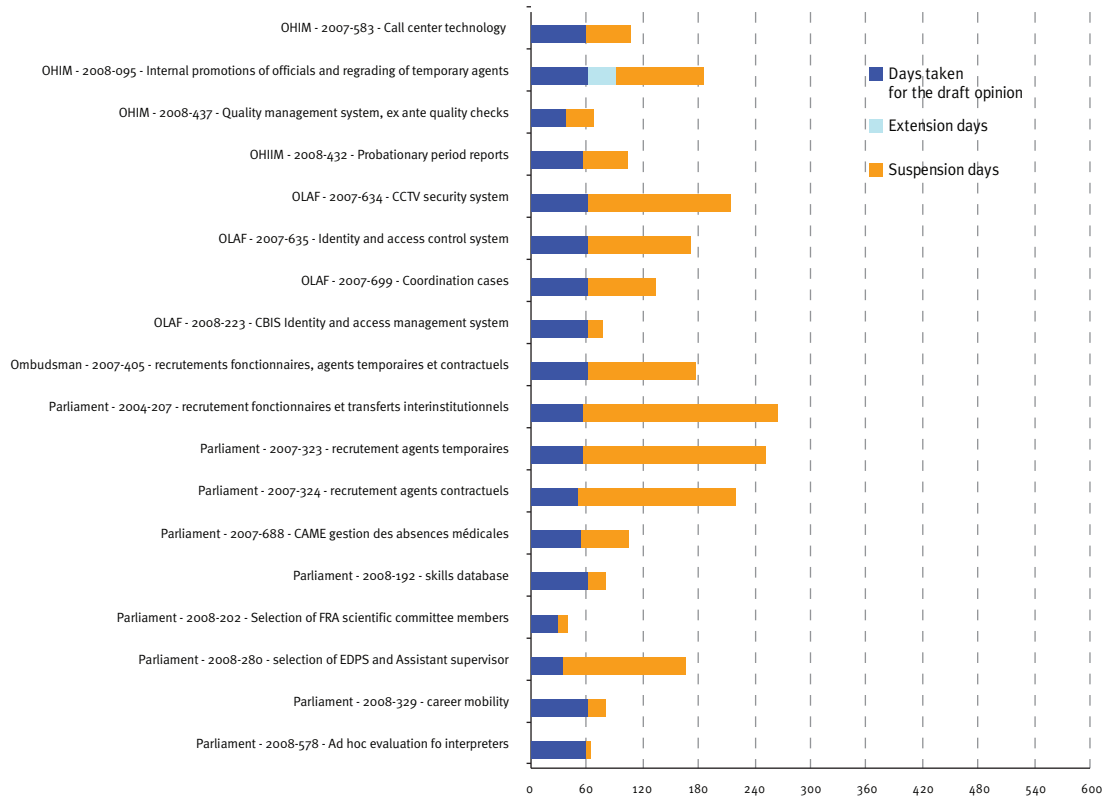
Opinions issued in 2008 (I)



Opinions issued in 2008 (2)



**Opinions issued in 2008 (3)**



NB: Days taken for the draft opinions do not include the month of August in ex-post cases received before 1/09/08. Suspension days include the suspension for comments on the draft, normally 7 to 10 days.

## Annex F

## List of prior-check opinions

**Database ARDOS — Commission**

Opinion of 15 December 2008 on a notification for prior checking regarding the database ARDOS (Case 2007-380)

**'Leadership feedback' — Commission**

Opinion of 15 December 2008 on the notification for prior checking regarding the optional 'Leadership Feedback' procedure established by the European Administrative School ('EAS') in connection with its management courses (Case 2008-527)

**Enquêtes du Bureau de sécurité — Conseil**

Avis du 12 décembre 2008 sur la notification à propos de la conduite des enquêtes du Bureau de sécurité (Dossier 2008-410)

**Appels d'offres — Banque européenne d'investissements**

Avis du 5 décembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Appels d'offres' (Dossier 2007-126)

**Evaluation of interpreters — Parliament**

Opinion of 5 December 2008 on a notification for prior checking concerning the evaluation of interpreters (Case 2008-578)

**Trainee recruitment — Cedefop**

Opinion of 5 December 2008 on a notification for prior checking on trainee recruitment (Case 2008-196)

**Flexitime — Cour des comptes**

Avis du 5 décembre 2008 sur la notification d'un contrôle préalable à propos du traitement des données 'Système de gestion et de contrôle du Flexitime' (Dossier 2008-173)

**IRIS: allocations familiales — Commission**

Avis du 5 décembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'IRIS: allocations familiales' (Dossier 2008-439)

**COMPAS — Commission**

Opinion of 4 December 2008 on a notification for prior checking regarding the 'Coordination of medical, psychosocial and administrative support (COMPAS)' (Case 2008-428)

**Certification — Comité économique et social**

Avis du 26 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Procédure de certification' (Dossier 2008-475)

**Aide complémentaire aux handicapés — Conseil**

Avis du 25 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Aide complémentaire aux handicapés' (Dossier 2008-388)

**Probationary period reports — OHIM**

Opinion of 25 November 2008 on a notification for prior checking concerning 'Probationary Period Reports' (Case 2008-432)

**Attestation — Comité économique et social**

Avis du 25 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'procédure d'attestation' (Dossier 2008-476)

**Promotion — Cour des comptes**

Avis du 24 novembre 2008 sur la notification de contrôle préalable à propos du dossier 'procédure de promotion' (Dossier 2007-292)

**Enregistrement des appels au dispatching technique — Commission**

Avis du 19 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles' (Dossier 2008-491)

**Mise en invalidité — Comité économique et social**

Avis du 19 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Procédure de mise en invalidité' (Dossier 2008-555)

**Dossiers médicaux individuels — Commission**

Avis du 18 novembre 2008 sur la notification d'un contrôle préalable à propos de la 'gestion des dossiers médicaux individuels Bruxelles — Luxembourg' (Dossier 2004-225)

**Selection of managers — OHIM**

Opinion of 12 November 2008 on a notification for prior checking regarding the selection of managers (Case 2008-435)

**Absence pour maladie ou accident — Conseil**

Avis du 11 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Procédure en cas d'absence pour maladie ou accident' (Dossiers 2008-271 et 2008-283)

**Expert database — EFSA**

Opinion of 11 November 2008 on the notification for prior checking regarding EFSA's Expert Database (Case 2008-455)

**Internet monitoring — Court of Auditors**

Opinion of 10 November 2008 on a notification for prior checking related to Internet monitoring (Case 2008-284)

**Promotion of officials and regrading of temporary agents — OHIM**

Opinion of 7 November 2008 on the notification for prior checking regarding the internal promotion of officials and regrading of temporary agents (Case 2008-95)

**Radiation exposure — Commission**

Opinion of 5 November 2008 on the notification for prior checking regarding occupational radiation exposure data (Case 2007-385)

**Infractions routières — Commission**

Avis du 3 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'infractions routières avec les véhicules officiels de la Commission gérés par l'Office Infrastructures et Logistique de Bruxelles (OIB)' (Dossier 2008-395)

**eHest training — Council**

Opinion of 22 October 2008 on the notification for prior checking regarding eHEST training (Computer based Hostile Environment Security Training) (Case 2008-387)

**Quality checks — OHIM**

Opinion of 22 October 2008 on the notification for prior checking regarding quality checks (Case 2008-437)

**Selection of EDPS and Assistant Supervisor — European Parliament and Council**

Opinion of 21 October 2008 on the selection of European Data Protection Supervisor and Assistant Supervisor (Cases 2008-280 and 2008-292)

**Recording of Emergency calls at the JRC ISPRA site — Commission**

Letter of 13 October 2008 in reply to a notification for prior checking concerning the 'Recording of emergency calls at the JRC ISPRA site' (Case 2008-492)

**Grantholders at JRC — Commission**

Opinion of 9 October 2008 on a notification for prior checking on the selection, recruitment and management of grantholders at the Joint Research Centre (JRC) (Case 2008-138)

**Trainees at the JRC — Commission**

Opinion of 9 October 2008 on a notification for prior checking on the trainee selection procedure and management of trainees at the Joint Research Centre (JRC) (Case 2008-136)

**Recruitment procedure for contract agents at the JRC — Commission**

Opinion of 9 October 2008 on a notification for prior checking regarding the recruitment procedure for contract agents at the Joint Research Centre (Case 2008-142)

**Recruitment files for officials at the JRC — Commission**

Opinion of 9 October 2008 on the notification for prior checking regarding the 'Management of recruitment files for officials at the JRC (transfers and laureates of open competitions)' (Case 2008-140)

**Enquêtes en matière de sécurité — Commission**

Avis du 2 octobre 2008 sur une notification de contrôle préalable à propos des enquêtes en matière de sécurité (Dossier 2007-736)

**Pilot project on individual productivity monitoring — Council**

Opinion of 1 October 2008 on a notification for prior checking on a pilot project on individual productivity monitoring: further processing of personal data in Workflow (Case 2008-436)

**Réseau de personnes de confiance (harcèlement) — Commission**

Avis du 30 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'mise en œuvre par le service gestionnaire et le réseau des personnes de confiance de la procédure informelle de lutte contre le harcèlement moral et le harcèlement sexuel à la Commission européenne (procédure contre le harcèlement) (Dossier 2008-062)

**Recruitment of trainees — EMSA**

Opinion of 29 September 2008 on a notification for prior checking regarding 'recruitment of trainees within the traineeship scheme in EMSA' (Case 2008-384)

**Double allocation pour enfant à charge — Conseil**

Avis du 29 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Double allocation pour enfant à charge en cas de handicap' (Dossier 2008-405)

**Stage — Cour des comptes**

Avis du 19 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'demandes de stage rémunéré ou non-rémunéré' (Dossier 2008-391)

**Career mobility — Parliament**

Opinion of 17 September 2008 on a notification for prior checking regarding the 'Career Mobility' (Case 2008-329)

**Sous-traitance de la caisse de maladie — BEI**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'sous-traitance partielle de a caisse de maladie' (Dossier 2008-323)

**Accréditation des journalistes — Conseil**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable sur l'accréditation de journalistes participant aux réunions du Conseil européen (Dossier 2004-259)

**Accréditation du personnel des firmes externes — Conseil**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable sur l'accréditation du personnel des firmes externes participant aux réunions du Conseil européen (Dossier 2007-046)

**Interface Flexitime/PersonaGrata — Conseil**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier 'Interface Flexitime — PersonaGrata (DGA3) (Dossier 2008-324)

**Calls for tenders and contracts — CoR and EESC**

Opinion of 15 September 2008 on a notification for prior checking regarding the processing operations to manage calls for tenders and contracts (Case 2008-346)

**Flexitime interface to TIM at Enterprise and Industry DG — Commission**

Answer of 15 September 2008 to a notification for prior checking relating to the Enterprise and Industry DG flexitime interface to TIM (Case 2008-111)

**Dosimetry management system — Commission**

Opinion of 3 September 2008 on a notification for prior checking on 'Dosimetry management system of radiological workers at JRC-IE in Petten' (Case 2008-020)

**Security investigations at Ispra — Commission**

Opinion of 31 July 2008 on a notification for prior checking on the security investigations at Joint Research Centre ISPRA (Case 2007-507)

**Service conjoint médico-social — CdR et CESE**

Avis du 4 juillet 2008 sur la notification d'un contrôle préalable à propos du dossier 'service conjoint médico-social' (Dossier 2007-004)

**Identity and access management system — OLAF**

Opinion of 30 June 2008 on a notification for prior checking on CBIS identity and access management system (Case 2008-223)



**Day care centre — Cedefop**

Opinion of 20 June 2008 on a notification for prior checking on the 'Day care centre' case (Case 2008-193)

**Recruitment — EMCDDA**

Opinion of 20 June 2008 on the notification for prior checking concerning the staff recruitment (Case 2008-157)

**Leave and flexitime — EMCDDA**

Opinion of 20 June 2008 on a notification for prior checking on the management of leave and flexitime (Case 2008-158)

**Recruitment — European Medicines Agency**

Opinion of 19 June 2008 on the notification for prior checking regarding EMEA's 'Access' recruitment database and selection and recruitment procedures (Case 2007-422)

**Early retirement — EMCDDA**

Opinion of 16 June 2008 on the notification for prior checking on the annual exercise for early retirement without reduction of pension rights (Case 2008-154)

**Skills database — Parliament**

Opinion of 13 June 2008 on the notification for prior checking regarding the skills database (Case 2008-192)

**Selection and management of interim staff at JRC — Commission**

Opinion of 9 June 2008 on a notification for prior checking regarding the selection and management of interim staff at JRC (Case 2008-139)

**Medical check-ups — CPVO**

Opinion of 4 June 2008 on the notification for prior checking regarding CPVO's pre-employment and annual medical check-ups (Case 2007-176)

**Parking pour les personnes à mobilité réduite — Conseil**

Avis du 29 mai 2008 sur la notification d'un contrôle préalable à propos du dossier de l'attribution et la réservation de places de parking aux personnes à mobilité réduite (PMR) (Dossier 2007-753)

**Assignment of ALER flats — Commission**

Opinion of 26 May 2008 on a notification for prior checking on assignment of ALER flats to statutory staff of JRC Ispra and the European School in Varese (Case 2008-144)

**JRC-IRMM Childcare facility (Crèche) in Geel — Commission**

Opinion of 23 May 2008 on a notification for prior checking regarding the processing operations on personal data concerning 'JRC-IRMM Childcare Facility (Crèche) in Geel' (Case 2008-152)

**Third language — EMCDDA**

Opinion of 20 May 2008 on a notification for prior checking on the evaluation of staff's capacity to work in a third language (Case 2008-159)

**CCTV System — OLAF**

Opinion of 19 May 2008 on the notification for prior checking regarding OLAF's CCTV system (Case 2007-634)

**Selection of candidates for the positions of EDPS and Assistant Supervisor — Commission**

Opinion of 16 May 2008 on a notification for prior checking on the selection of candidates in order to establish a short-list for the position of European Data Protection Supervisor and the position of Assistant Supervisor (Case 2008-222)

**Selection procedure of Agency's Scientific Committee — FRA**

Opinion of 29 April 2008 on a notification for prior checking on the selection procedure of members of the Agency's Scientific Committee (Joint Cases 2008-179 and 2008-202)

**Personnes de confiance dans le cadre du harcèlement — Commission**

Avis du 29 avril sur la notification de contrôle préalable à propos du dossier 'Sélection des personnes de confiance dans le cadre de la lutte contre le harcèlement moral et le harcèlement sexuel à la Commission européenne' (Dossier 2008-60)

**Childcare facilities at JRC Ispra — Commission**

Opinion of 21 April 2008 on a notification for prior checking regarding the 'Administration of JRC Ispra childcare facilities (crèche / garderie) (Case 2007-544)

**Family leave — EMEA**

Opinion of 14 April 2008 on a notification for prior checking concerning the 'Family leave / Compel personnel database / Electronic document management system (EDMS)' (Case 2007-498)

**Annual appraisal procedure — CPVO**

Opinion of 14 April 2008 on a notification for prior checking on the annual appraisal procedure (Case 2007-403)

**Identity and access control system — OLAF**

Opinion of 7 April 2008 on a notification for prior checking on identity and access control system (Case 2007-635)

**Coordination cases — OLAF**

Opinion of 7 April 2008 on a notification for prior checking on coordination cases (Case 2007-699)

**Part time requests — European Medicines Agency**

Opinion of 1 April 2008 on a notification for prior checking on part time requests (Case 2007-500)

**Autorisations de témoigner en justice — Commission**

Avis du 28 mars 2008 sur la notification d'un contrôle préalable à propos du dossier 'Autorisations de témoigner en justice' (Dossier 2007-721)

**Départ à la retraite sans réduction des droits — Cour de justice**

Avis du 17 mars 2008 sur la notification de contrôle préalable à propos du dossier 'départ à la retraite sans réduction des droits à pension' (Dossier 2007-579)

**Recrutement des fonctionnaires et transferts interinstitutionnels — Parlement**

Avis du 13 mars 2008 sur la notification d'un contrôle préalable à propos du dossier 'recrutement des fonctionnaires et transferts interinstitutionnels' (Dossier 2004-207)

**Recrutement des agents temporaires — Parlement**

Avis du 13 mars 2008 sur la notification d'un contrôle préalable à propos du dossier 'recrutement des agents temporaires' (Dossier 2007-323)

**Recrutement des agents contractuels — Parlement**

Avis du 13 mars 2008 sur la notification d'un contrôle préalable à propos du dossier 'recrutement des agents contractuels' (Dossier 2007-384)

**Evaluation d'un handicap — Conseil**

Avis du 7 mars 2008 sur la notification d'un contrôle préalable à propos du dossier 'formulaire d'évaluation d'un handicap' (Dossier 2008-17)

**Activités de l'Ecole européenne d'administration et d'EPSO dans le cadre de la certification — Commission**

Avis du 7 mars 2008 sur la notification d'un contrôle préalable à propos du dossier 'Activités de l'Ecole européenne d'administration et d'EPSO dans le cadre de la procédure de certification' (Dossier 2006-396)

**Gestion des absences médicales — Parlement**

Avis du 4 mars 2008 sur la notification d'un contrôle préalable à propos du dossier 'CAME — gestion des absences médicales' (Dossier 2007-688)

**Promotion of temporary agents — EMEA**

Opinion of 20 February 2008 on a notification for prior checking on the promotion of temporary agents (Case 2007-418)

**Control system by an iris scan — European Central Bank**

Opinion of 14 February 2008 on a notification for prior checking related to the extension of a pre-existing access control system by an iris scan technology for high secure business areas (Case 2007-501)

**Administrative enquiries and disciplinary proceedings — Cedefop**

Opinion of 13 February 2008 on a notification for prior checking on the data processing carried out in the framework of administrative enquiries and disciplinary proceedings (Case 2007-582)

**Checks on absences at JRC Ispra and Seville — Commission**

Opinion of 6 February 2008 on the notification for prior checking regarding the 'checks on absences from work due to illness or accident — Directorate-General Joint Research Centre Ispra and Seville' dossier (Case 2007-508)

**Dosimetry management system — Commission**

Opinion of 6 February 2008 on a notification for prior checking concerning the Dosimetry Management System at DG JRC Ispra (Case 2007-505)

**Identity management service — Commission**

Opinion of 6 February 2008 on a notification for prior checking related to the Identity Management Service (Case 2007-349)

**Candidats au télétravail — Commission**

Avis du 6 février 2008 sur la notification de contrôle préalable à propos du dossier 'Sélection du personnel candidat au télétravail' (Dossier 2007-720)

**Individual medical files at JRC — Commission**

Opinion of 6 February 2008 on a notification for prior checking on individual medical files at Joint Research Centre in Ispra and Seville (Case 2007-329)

**Career development & appraisal cycle — EFSA**

Opinion of 25 January 2008 on a notification for prior checking concerning 'Career development and appraisal cycle' (Case 2007-585)

**CASABLANCA — Conseil**

Avis du 25 janvier 2008 sur la notification de contrôle préalable à propos du dossier 'CASABLANCA (gestion des actions de formation professionnelle)' (Dossier 2007-584)

**Medical examinations at JRC in Ispra — Commission**

Opinion of 25 January 2008 on 'First aid, accidents at work and other medical examinations' at JRC (Joint Research Centre) in Ispra (Case 2007-372)

**Procédure d'embauche — Conseil**

Avis du 25 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier 'Procédure d'embauche des fonctionnaires et autres agents du Secrétariat général du Conseil' (Dossier 2007-194)

**Occupational medicine — Commission**

Opinion of 23 January 2008 on a notification for prior checking concerning the Occupational Medicine (MeDeL) at DG JRC (Case 2007-504)

**PowerLab Management — Commission**

Opinion of 17 January 2008 on a notification for prior checking concerning the management of clinical and toxicological laboratories environment (PowerLab) at DG JRC (Case 2007-649)

**Contrat de traducteur freelance — Centre de traduction**

Avis du 17 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier 'appel d'offre et passation d'un contrat avec un traducteur freelance' (Dossier 2007-327)

**Dossiers médicaux des enfants de la crèche — Conseil**

Avis du 17 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier 'Gestion des dossiers médicaux des enfants fréquentant la Crèche du Secrétariat Général du Conseil (SGC)' (Dossier 2007-491)

**Staff evaluation — EMCDDA**

Opinion of 11 January 2008 on a notification for prior checking concerning the 'Staff evaluation / assessment exercise' (Case 2007-334)

**Call centre technology — OHIM**

Opinion of 11 January 2008 on a notification for prior checking on the call centre technology (Case 2007-583)

**E-tendering — Council**

Opinion of 10 January 2008 on a notification on e-Tendering application covering the Council's public procurement procedures (Case 2007-573)

**AGS-EDV Database at JRC-ITU in Karlsruhe — Commission**

Opinion of 10 January 2008 on a notification for prior checking on 'AGS-EDV Database at JRC-ITU in Karlsruhe' (Case 2007-378)

**Recrutements — Médiateur européen**

Avis du 9 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier 'Recrutements des membres du personnel (fonctionnaires / temporaires / contractuels)' (Dossier 2007-405)

**Probationary period reports — European Maritime Safety Agency**

Opinion of 7 January 2008 on a notification for prior checking concerning 'probationary period reports' (Case 2007-569)

**Recording of leave — European Medicines Agency**

Opinion of 7 January 2008 on a notification for prior checking on recording of the leave of temporary, auxiliary and contract agents, national experts and trainees (Case 2007-420)

**Promotion — Comité des Régions**

Avis du 7 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier 'Procédure de promotion des fonctionnaires' (Dossier 2007-354)

**Recruitment — European Maritime Safety Agency**

Opinion of 7 January 2008 on a notification for prior checking regarding the 'recruitment of permanent, temporary and contract agents' (Case 2007-566)

## Annex G

# List of opinions on legislative proposals

### **European e-justice strategy**

Opinion of 19 December on the Commission communication on a European e-justice strategy

### **Cross-border healthcare**

Opinion of 2 December 2008 on the proposal for a directive on the application of patient's rights in cross-border healthcare

### **EU–US high-level contact group on information sharing**

Opinion of 11 November 2008 on the final report by the EU–US high-level contact group on information sharing and privacy and personal data protection

### **Transparency of debtors' assets**

Opinion of 22 September 2008 on the Commission Green Paper on the effective enforcement of judgements in the European Union: the transparency of debtors' assets — COM(2008) 128 final

### **ECRIS**

Opinion of 16 September 2008 on the proposal for a Council Decision on the establishment of the European Criminal Record Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA

### **Public access to documents**

Opinion of 30 June 2008 on the proposal for a regulation regarding public access to European Parliament, Council and Commission documents (OJ C 2, 7.1.2009, p. 7)

### **Protecting children using the Internet**

Opinion of 23 June 2008 on the proposal for a decision establishing a multiannual Community programme on protecting children using the Internet and other communication technologies (OJ C 2, 7.1.2009, p. 2)

### **European Statistics**

Opinion of 20 May 2008 on the proposal for a regulation on European statistics (COM(2007) 625 final) (OJ C 308, 3.12.2008, p. 1)

### **Road safety**

Opinion of 8 May 2008 on the proposal for a directive of the European parliament and of the Council facilitating cross-border enforcement in the field of road safety (OJ C 310, 5.12.2008, p. 9)

### **Eurojust**

Opinion of 25 April 2008 on the initiative with a view to adopting a Council decision concerning the strengthening of Eurojust and amending Decision 2002/187/JHA (OJ C 310, 5.12.2008, p. 1)

**Computerised reservation systems**

Opinion of 11 April 2008 on the proposal for a regulation on a code of conduct for computerised reservation systems (OJ C 233, 11.9.2008, p. 1)

**E-privacy**

Opinion of 10 April 2008 on the proposal for a directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications) (OJ C 181, 18.7.2008, p. 1)

**Security features and biometrics in passports**

Opinion of 26 March 2008 on the proposal for a regulation amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ C 200, 6.8.2008, p. 1)

**Internal Market Information System (IMI)**

Opinion of 22 February 2008 on the Commission Decision of 12 December 2007 concerning the implementation of the internal market information system (IMI) as regards the protection of personal data (2008/49/EC) (OJ C 270, 25.10.2008, p. 1)

## Annex H

## Composition of the EDPS's Secretariat

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

Sophie LOUVEAUX  
Administrator/Legal Officer  
Coordinator DPO Relations and Prior Checks

Delphine HAROU (\*)  
Supervision Assistant

Rosa BARCELÓ  
Administrator/Legal Officer

Xanthi KAPSOSIDERI  
Supervision Assistant

Zsuzsanna BELENYESSY  
Administrator/Legal Officer

Sylvie LONGRÉE  
Supervision Assistant

Eva DIMOVNÉ KERESZTES  
Administrator/Legal Officer  
Coordinator Inspections

Kim Thien LÊ  
Secretariat Assistant

Maria Veronica PEREZ ASINARI  
Administrator/Legal Officer  
Coordinator Administrative Measures

Thomas Gremel  
Supervision Assistant

Jaroslav LOTARSKI  
Administrator/Legal Officer  
Coordinator Complaints

György HALMOS (\*)  
National Expert/Legal Officer  
(until September 2008)

Tereza STRUNCOVA  
Administrator/Legal Officer

Athena BOURKA  
National Expert / Technology Officer  
(since September 2008)

Isabelle CHATELIER  
Administrator/Legal Officer

Manuel GARCIA SANCHEZ  
National Expert/Technology Officer  
(since Sept. 2008)

• **Policy and information**

Hielke HIJMANS,  
Administrator/Legal Officer  
Coordinator Consultation and Court Procedures

Nathalie VANDELLE (\*)  
Administrator/Press Officer  
Coordinator Information team

Laurent BESLAY  
Administrator Technology Officer  
Coordinator Security and Technology

Martine BLONDEAU (\*)  
Documentation Assistant

Bénédicte HAVELANGE  
Administrator/Legal Officer  
Coordinator Large IT Systems and Border Policy

Andrea BEACH  
Secretariat Assistant

Alfonso SCIROCCO  
Administrator/Legal Officer

Francisco Javier MOLEÓN GARCIA  
Documentation Assistant

Michaël VANFLETEREN  
Administrator/Legal Officer

Gerard VAN BALLEGOIJ  
Trainee (Oct. 2008 to Feb. 2009)

Anne-Christine Lacoste  
Administrator/Legal Officer  
Coordinator Article 29 Working Party

Athina FRAGKOULI  
Trainee (Oct. 2008 to Feb. 2009)

Herke KRANENBORG  
Administrator/Legal Officer

Sarah THOME  
Trainee (Oct. 2008 to Feb. 2009)

Katarzyna CUADRAT-GRZYBOWSKA  
Administrator/Legal Officer

(\*) 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**

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

Anne LEVÉCQUE  
*Human Resources Assistant*

Vittorio MASTROJENI  
*Human Resources Assistant*

- **Budget and finance**

Tonny MATHIEU  
*Finance Administrator*

Maria SANCHEZ LOPEZ  
*Finance and Accounting Assistant*

Raja ROY  
*Finance and Accounting Assistant*

- **Administration**

Anne-Françoise REYNDERS  
*Social activities, Infrastructure, Administration 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 (24/6/2004). 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 and Employment, Social Affairs and Employment, Social Affairs and Equal Opportunities DG)
- Service-level agreement with the Council
- Service-level agreement with the European Administrative School (EAS)
- Administrative Arrangement between the European Data Protection and the European Network and Information Security Agency (ENISA)
- Agreement on the harmonisation of the cost of the inter-institutional language courses
- Bilateral agreements between the European Parliament and the EDPS implementing the administrative agreement of 24/06/2004, prolonged the 11/12/2006.

### 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 the Staff Regulations on transfer of pension rights

Decision of 1 October 2007 of the Supervisor for implementing Article 22(4) of Annex XIII of the 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

Rules of 16 June 2008 on the reimbursement of expenses incurred by persons from outside the EDPS's services invited to attend meetings in an expert capacity

Decision of 8 August 2008 of the authorising officer, by delegation, related to the archiving of financial and supporting documents;

Decision of 2 October 2008 of the Supervisor regarding general implementing rules of Article 45a of the Staff Regulations (Certification)

Decision of 16 December 2008 of the Supervisor adopting security measures within the EDPS

Decision of 19 December 2008 of the Supervisor on the appointment of a local Security Officer for the EDPS

European Data Protection Supervisor

**Annual Report 2008**

Luxembourg: Office for Official Publications of the European Communities

2008 — 130 pp. — 21 × 29.7 cm

ISBN 978-92-95073-02-9

doi: 10.2804/55407



### **How to obtain EU publications**

#### **Publications for sale:**

- via EU Bookshop (<http://bookshop.europa.eu>);
- from your bookseller by quoting the title, publisher and/or ISBN number;
- by contacting one of our sales agents directly. You can obtain their contact details on the Internet (<http://bookshop.europa.eu>) or by sending a fax to +352 2929-42758.

#### **Free publications:**

- via EU Bookshop (<http://bookshop.europa.eu>);
- at the European Commission's representations or delegations. You can obtain their contact details on the Internet (<http://ec.europa.eu>) or by sending a fax to +352 2929-42758.



EUROPEAN DATA  
PROTECTION SUPERVISOR

*The European guardian  
of personal data protection*

**[www.edps.europa.eu](http://www.edps.europa.eu)**



Publications Office



9 789295 073029

ISBN 978-92-95073-02-9