

Annual Report

2005



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.

A great deal of additional information on the European Union is available on the Internet. It can be accessed through the Europa server (<http://europa.eu.int>).

Cataloguing data can be found at the end of this publication.

Luxembourg: Office for Official Publications of the European Communities, 2006

ISBN 92-95030-00-1

© European Communities, 2006

Reproduction is authorised provided the source is acknowledged.

Printed in Luxembourg

PRINTED ON WHITE CHLORINE-FREE PAPER

Contents

User guide	8
Mission statement	10
Foreword	11
1. Balance and perspectives	13
1.1. General overview of 2005	13
1.1.1. Supervision	14
1.1.2. Consultation	15
1.1.3. Cooperation	17
1.1.4. Communication	18
1.1.5. Resources	18
1.2. Legal framework	19
1.2.1. Background	20
1.2.2. Regulation (EC) No 45/2001	21
1.2.3. Tasks and powers of the EDPS	22
1.3. Results in 2005	23
1.4. Objectives for 2006	25
2. Supervision	27
2.1. General	27
2.2. Data protection officers	28
2.3. Prior checks	30
2.3.1. Legal base	30
2.3.2. Procedure	31
2.3.3. Quantitative analysis	34
2.3.4. Main issues in <i>ex post</i> cases	40
2.3.5. Main issues in proper prior checks	41
2.3.6. Consultations	42
2.3.7. Follow-up of prior-check opinions and consultations	43
2.3.8. Conclusions and future	45
2.4. Complaints	46
2.4.1. Introduction	46
2.4.2. Cases declared admissible	47
2.4.3. Cases not declared admissible: main reasons for inadmissibility	49
2.4.4. Collaboration with the Ombudsman	49

2.4.5. Further work in the field of complaints	50
2.5. Investigations	50
2.6. Public access to documents and data protection	50
2.7. E-monitoring	52
2.8. Eurodac	52
3. Consultation	54
3.1. Introduction	54
3.2. The policy of the EDPS	56
3.3. Legislative proposals.....	59
3.3.1. The opinions of the EDPS in 2005	59
3.3.2. Horizontal themes	64
3.4. Other activities in the area of consultation.....	66
3.4.1. Related documents.....	66
3.4.2. Interventions before the Court of Justice.....	66
3.4.3. Administrative measures	67
3.5. Perspectives for 2006 and further	68
3.5.1. New technological developments	68
3.5.2. New developments in policy and legislation	71
4. Cooperation.....	74
4.1. Article 29 Working Party	74
4.2. Third pillar	76
4.3. European conference.....	79
4.4. International conference.....	80
4.5. Workshop for international organisations.....	81
5. Communication.....	81
5.1. Introduction.....	81
5.2. Main activities and target groups	82
5.3. Communication tools	84
5.4. The EDPS information campaign	84
5.5. The press service.....	84
5.6. The website	85
5.7. Speeches.....	85
5.8. Newsletter	87
5.9. Information.....	87

5.10. Logo and house style.....	88
5.11. Visits	89
6. Administration, budget and staff.....	89
6.1. Introduction: continuing to establish the new institution	89
6.2. Budget	90
6.3. Human resources.....	90
6.3.1. Recruitment.....	91
6.3.2. Traineeships programme	92
6.3.3. Programme for seconded national experts.....	93
6.3.4. Organisation chart.....	94
6.3.5. Training.....	94
6.4. Consolidation of cooperation	94
6.4.1. Follow-up to the administrative cooperation agreement	94
6.4.2. Interinstitutional cooperation.....	96
6.4.3. External relations	96
6.5. Infrastructure	96
6.6. Administrative environment	97
6.6.1. Establishment of internal control standards.....	97
6.6.2. Setting up of the interim staff committee at the EDPS	97
6.6.3. Flexitime	98
6.6.4. Internal rules	98
6.7. Objectives for 2006.....	98
Annexes.....	100
Annex A — Extract from Regulation (EC) No 45/2001	101
Annex B — List of abbreviations.....	103
Annex C — List of data protection officers	104
Annex D — Prior-checking handling time per case and per institution.....	106
Annex E — List of prior-check opinions	109
Annex F — List of opinions on legislative proposals	113
Annex G — Composition of the EDPS Secretariat.....	114
List of service-level agreements signed by the EDPS with the other institutions	116
List of decisions adopted by the EDPS	116

USER GUIDE

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

Chapter 1 — **Balance and perspectives** presents a general overview of the activities of the EDPS, also detailing the relevant legal framework. In addition, the chapter highlights results achieved in 2005 and puts forth objectives for 2006.

Chapter 2 — **Supervision** extensively describes the work carried out to ensure and monitor that the EU institutions and bodies comply with their data protection obligations. A general overview is followed by an analysis of the role of the data protection officers (DPO) in the EU administration. This chapter includes an analysis of prior checks, complaints and investigations treated in 2005, as well as the main findings of a paper on transparency and public access, published in July. It also includes a section on e-monitoring and an update on the central unit of Eurodac.

Chapter 3 — **Consultation** deals with the EDPS's advisory role, focusing on a policy paper published in March, and on opinions on legislative proposals and related documents, as well as on their impact. The chapter also contains an analysis of horizontal themes and introduces some new technological developments — such as the use of biometrics and radio frequency identification (RFID).

Chapter 4 — **Cooperation** describes the work carried out in key forums such as the Article 29 Working Party, in the joint supervisory authorities of the 'third pillar', and at the European as well as the International Data Protection Conference. A report on a workshop organised for international organisations closes the chapter.

Chapter 5 — **Communication** presents the information strategy and the use of different communication tools, such as the website, newsletters, the press service and speeches.

Chapter 6 — **Resources** contains a description of how the EDPS's office was consolidated during the second year of business, running through budget issues, human resources questions and administrative agreements.

The report is completed by **annexes**, which contain relevant extracts of Regulation (EC) No 45/2001, a list of abbreviations, statistics for prior checks, the list of DPOs of institutions and bodies, a description of the composition of the secretariat, etc.

A separate **executive summary** has been published for those who prefer the short version of the main developments of 2005.

Those wanting to find out more about the EDPS are encouraged to visit our website, which remains our primary tool of communication (www.edps.eu.int).

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

MISSION STATEMENT

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

- monitoring and ensuring that the provisions of Regulation (EC) No 45/2001, as well as other Community acts on the protection of fundamental rights and freedoms, are complied with when Community institutions and bodies process personal data (supervision);
- advising the Community institutions and bodies on all matters relating to the processing of personal data, including 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 European Union, 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 Community institutions and bodies, thereby also contributing to improving ‘good governance’;
- integrate respect for ‘data protection principles’ in Community legislation and policies, whenever relevant;
- improve the quality of EU policies, whenever ‘effective data protection’ is a basic condition for their success.

FOREWORD

I have the pleasure to submit a second 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 2005 as the first full year of activity in the existence of the EDPS as a new independent supervisory authority, with the task of ensuring that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data are respected by the Community institutions and bodies.

The decision of the European Parliament and the Council appointing me as European Data Protection Supervisor and Joaquín Bayo Delgado as Assistant Supervisor entered into effect on 17 January 2004. Therefore, most of 2004 was required to make the first crucial steps in the ‘building of a new institution’ and the development of its strategic roles at Community level, to monitor and ensure the application of legal safeguards for the protection of the personal data of citizens of the European Union.

We are very pleased that one of the central messages in the first annual report — i.e. that protection of personal data, as a fundamental value underlying EU policies, should be considered as a condition for the success of those policies — has been received well and, more importantly, acted upon by different stakeholders. It was also recognised that such action had become a matter of urgency, since the EU cannot afford not to deliver on the rules it has imposed on itself and on the Member States.

This is no doubt one of the reasons why we have been able to make substantial progress in the course of 2005 striving to further developing our strategic roles and consolidating the position of the EDPS as a new authoritative and visible player in a highly relevant area. This annual report explains these different roles in more detail and offers clear evidence of their growing impact.

Let me therefore take this opportunity, once again, to thank those in the European Parliament, the Council and the Commission who have actively contributed to our successful start and who continue to support our work, as well as those in different institutions and bodies with whom we closely collaborate and who are most often directly responsible for the way in which data protection is ‘delivered’ in practice.

I want to express special thanks to the members of our staff that take part in our mission and continue to make a major difference in its results. The level of quality and dedication that we have enjoyed in the staff has been outstanding and has contributed more than anything else to our growing effectiveness. A modest increase in the size of the staff has also been crucial and most welcome, and this will continue to be so in the near future.

Peter Hustinx

European Data Protection Supervisor

1. BALANCE AND PERSPECTIVES

1.1. General overview of 2005

The legal framework within which the European Data Protection Supervisor (EDPS) acts — see further in paragraph 1.2 — has resulted in a number of tasks and powers, which allow a basic distinction between three main roles. These strategic roles have been taken as starting points for the new authority and will continue to serve as guidelines in the near future:

- a **supervisory** role, to monitor and ensure that Community institutions and bodies 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 (police and judicial cooperation in criminal matters), with a view to improving consistency in the protection of personal data.

These roles will be elaborated in Chapters 2, 3 and 4 of this annual report, in which a presentation of the main activities of the EDPS and the progress achieved in 2005 is given. The crucial importance of information and communication about these activities has led to a separate emphasis on **communication** in Chapter 5. Most of these activities rely on effective management of financial, human and other **resources**, as will be discussed in Chapter 6. The main roles of the EDPS are reflected in the mission statement.

It is important at this point to emphasise again that **more and more EU policies depend on the lawful processing of personal data**. Many public or private activities in a modern society nowadays generate personal data or use such data as input. This is also true for the European institutions and bodies in their administrative or policy-making roles, and for the implementation of their policy agenda. This means that **effective protection of personal data**, as a fundamental value underlying EU policies, should be seen as **a condition for their success**. The EDPS will continue to act in this general spirit and expects a positive response in return.

1.1.1. Supervision

A first emphasis has been put on the development of the network of **data protection officers** (DPOs) of institutions and bodies. In November 2005, a position paper was issued on the role of DPOs in ensuring effective compliance with Regulation (EC) No 45/2001. The position paper was sent to the heads of the EU administration and underlined the role of the DPO as a strategic partner for institutions and bodies in ensuring compliance. One of the key messages was that all bodies need to appoint a DPO as a vital first step on their way towards compliance. A second key message was that DPOs must be notified more adequately of personal data processing within their institution or body and notify the EDPS of any processing operation which entails specific risks for the people concerned and therefore need to be prior checked. The relation with DPOs is further discussed in paragraph 2.2 of this report.

A major second emphasis has been on the prior checking of processing operations which are likely to present specific risks for the data subjects, as mentioned in Article 27 of the regulation. Although this task was typically designed to deal with new processing operations, most prior checks have so far been ex post prior checks, due to the fact that many existing systems would have qualified for prior checking, had the EDPS been available at the time of their entering into operation. In 2005, 34 opinions were issued in prior-checking cases, 30 of which were on existing systems of various institutions and bodies. Other cases were consultations about the need for prior checking, or cases found not to be subject to prior checking which still gave reason for comments. The EDPS has defined a number of thematic priorities, which guide the prioritising of the prior checking, notably medical files, staff appraisal, disciplinary procedures, social services and e-monitoring. At the end of 2005, 29 notifications were in process and many more are expected in the near future. The institutions and bodies have been encouraged to submit their notifications for prior checking not later than by spring 2007. A further analysis of relevant criteria, procedural aspects, institutions and issues, and follow-up of prior-check opinions and consultations is presented in paragraph 2.3 of this report.

A third emphasis has been on the handling of **complaints**. However, in 2005, only five out of 27 complaints received by the EDPS were declared admissible and further examined. In practice, a large majority of complaints do not raise issues for which the EDPS is competent. In such cases, the complainant is informed in a general way and, if possible, advised on a more appropriate alternative. With respect to the handling of complaints within his competence, the EDPS has been in contact with the European Ombudsman to examine a potential scope for collaboration in the near future. More information about this subject is available in paragraph 2.4 of this report.

Considerable efforts have also been invested in the elaboration of a background paper on **public access to documents and data protection**, which was presented in July 2005 (see paragraph 2.6), the preparation of a background paper on the use of **electronic communications** (see paragraph 2.7), and to prepare various activities relating to the supervision of **Eurodac** (see paragraph 2.8).

1.1.2. Consultation

A first priority in this area has been the definition of a **policy on the role of the EDPS** as an advisor to the Community institutions on proposals for legislation and related documents. A policy paper was issued in March 2005, which emphasises that the advisory task has a wide scope and deals with all proposals for legislation with an impact on the protection of personal data. This interpretation has been confirmed by the Court of Justice. The policy paper also sets out the substantive approach which the EDPS intends to take to such proposals for legislation, as well as his procedural role in the different stages of the legislative process. The European Commission is making good use of the availability of the EDPS to make informal comments on a draft proposal before it is submitted for a formal consultation. A formal opinion is always published, often presented in a relevant committee in the European Parliament and/or the competent working party of the Council, and systematically followed on its way through the legislative process. This policy is further explained in paragraph 3.2 of this report.

The EDPS issued six formal **opinions** in 2005 which clearly reflect the relevant subjects on the policy agenda of the Commission, the Parliament and the Council. Important opinions related to the exchange of personal data in the third pillar, the development of large-scale information systems for VIS and the second generation of the Schengen information system (SIS II), and the highly controversial subject of the mandatory retention of data on electronic communications for access by law enforcement authorities. An analysis of these opinions and a few horizontal themes is presented in paragraph 3.3 of this report.

The EDPS has also, for the first time, made use of the possibility to **intervene in cases before the Court of Justice** which raise important questions of data protection. The Court has granted a request of the EDPS to be allowed to intervene in two cases before the Court on the transfer of passenger name record (PNR) data on airline passengers to the United States, in support of the conclusions of Parliament. The EDPS presented both written and oral observations, and is now looking forward to a decision of the Court in the two cases (see paragraph 3.4.2).

In the course of 2005, the EDPS also exercised his advisory role with respect to **administrative measures**, and more in particular on implementing rules of institutions and bodies in the area of data protection. This provides an important opportunity to influence, in a more structural fashion, the way in which data protection policies are implemented. In this context, the EDPS has developed an approach to the specific implementing rules concerning the role of DPOs (see paragraphs 2.2 and 3.4.3).

The EDPS has a special task in **monitoring new developments** that have an impact on the protection of personal data. This report therefore also presents an initial evaluation of some important new technological advances, and developments in policy and legislation that will be followed systematically in 2006 and thereafter (see paragraph 3.5).

1.1.3. Cooperation

A very important platform for cooperation with national supervisory authorities is the **Article 29 Working Party**, established by Article 29 of Directive 95/46/EC to advise the Commission and to develop harmonised data protection policies, of which the EDPS is a full member. A certain number of important proposals for legislation were covered by the EDPS and the working party in separate opinions. In these cases, the EDPS has welcomed the general support of national colleagues as well as additional comments which can lead to better protection of data. The EDPS has on the other hand also invested considerable efforts in the development of common positions which can contribute to more consistency and harmony in data protection law in the European Union (see paragraph 4.1).

Cooperation with **supervisory bodies in the third pillar** (such as the supervisory bodies for Schengen, customs, Europol and Eurojust) has concentrated to a large extent on the preparation of common positions with a view to the development of a much needed general framework for data protection in the third pillar of the EU. However, more specifically, discussions have taken place about a new system of supervision with regard to SIS II which will build on a close cooperation between national supervisory authorities and the EDPS (see paragraph 4.2). Each of these bodies has been established by a different instrument and is usually made up of representatives of national supervisory authorities.

The EDPS has also cooperated actively in the wider context of the **European and international conferences** of data protection commissioners (paragraphs 4.3 and 4.4). In September 2005, in cooperation with Council of Europe and OECD, the EDPS hosted a workshop on data protection in **international organisations** (paragraph 4.5).

1.1.4. Communication

In 2005, the EDPS paid specific attention to the development of an **information strategy** that can give adequate support to the strategic roles of the EDPS. Raising awareness about data protection generally, and about the roles and activities of the EDPS more specifically, is an important condition for effective supervision, consultation and cooperation. The information strategy has distinguished relevant target groups and relevant messages in relation to these different activities (see paragraph 5.2).

The EDPS has also invested in an enhancement of **information and communication tools**. A general information campaign in all EU institutions and bodies, and in all Member States, was followed up in 2005 by the introduction of a press service, a regular newsletter, the development of a new logo and house style, and will soon be completed by the introduction of a new website, which will be the most important tool of communication for the EDPS. Meanwhile, the EDPS has continued to provide useful information, both in response to specific requests and, generally, in opinions, papers and speeches at the present website (see paragraph 5.3 and beyond).

1.1.5. Resources

The EDPS has noted with satisfaction that the budget authorities have provided the **budgetary means** for consolidation and limited growth of the organisation, with due respect for the need to address urgent tasks in supervision and consultation on data protection in most institutions and bodies. The EDPS is aware of the importance of good financial management and budgetary rigour as conditions for continued trust in these matters (paragraph 6.2).

Major attention has been given to the development of **human resources**. Important results have been achieved, both in the general area of recruitment and in special programmes for trainees and secondment of national experts. A combination of different means has resulted in providing additional flexibility and continuous new challenges for the staff (paragraph 6.3).

It is difficult to overstate the importance of the **administrative agreement**, concluded in 2004 with the Commission, the Parliament and the Council, which has enabled the EDPS to benefit from outside support where appropriate, and to invest most resources in primary activities. A continuation of this agreement after three years is therefore essential. Other kinds of interinstitutional cooperation play an equally important role for an authority of such limited size and limited internal diversity as the EDPS (paragraph 6.4).

The gradual increase of staff and additional increases in the near future continue to highlight the importance of adequate **infrastructure** and housing (paragraph 6.5).

The administrative environment has also developed well in 2005. The adoption of **rules of procedure** will be an important milestone, with important consequences, both internally and externally, and has therefore been the subject of very careful preparation (paragraph 6.6).

1.2. Legal framework

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

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

1.2.1. 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 35 Member States of the Council of Europe, including all EU Member States.

Directive 95/46/EC was based on the principles of Convention 108, but specified and developed them in many ways. It aimed to provide a high level of protection and a free flow of personal data in the EU. When the Commission made the proposal for this directive in the early 1990s, it stated that Community institutions and bodies should be covered by similar legal safeguards, thus enabling them to take part in a free flow of personal data, subject to equivalent rules of protection. However, until the adoption of Article 286 of the EC Treaty, a legal basis for such an arrangement was lacking.

The appropriate rules referred to in Article 286 of the EC Treaty have been laid down in Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, which entered into force in 2001 ⁽¹⁾. 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 establishing a Constitution for Europe, signed in October 2004, places great emphasis on the protection of fundamental rights. Respect for private and family life and protection of personal data are treated as separate fundamental rights in Articles II-67 and II-68 of the Constitution. Data protection is also mentioned in Article I-51 of the Constitution, in Title VI on the ‘democratic life’ of the Union. This clearly indicates that data protection is now regarded as a basic ingredient of good governance. Independent supervision is an essential element of this protection.

⁽¹⁾ OJ L 8, 12.1.2001, p. 1

1.2.2. 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.

An interesting feature of the regulation is the obligation for Community institutions and bodies to appoint at least one person as a DPO. These officers have the task of ensuring the internal application of the provisions of the regulation, including the proper notification of processing operations, in an independent manner. All Community institutions and a number of bodies now have these officers, and some of them have been active for several years. This means that important work has been done to implement the regulation, even in the absence of a supervisory body. These officers may also be in a better position to advise or to intervene at an early stage and to help develop good practice. Since the DPO has the formal duty to cooperate with the EDPS, this is a very important and highly appreciated network to work with and to develop further (see paragraph 2.2).

1.2.3. Tasks and powers of the EDPS

The task and powers of the EDPS are clearly described in Articles 41, 46 and 47 of the regulation (see Annex A) 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. Monitoring relevant developments which may have an impact on the protection of personal data is also an important task. These **consultative** activities of the EDPS are more widely discussed in Chapter 3 of this report.

The duty to cooperate with national supervisory authorities and supervisory bodies in the third pillar, has a similar character. As a member of the Article 29 Working Party, established to advise the Commission and to develop harmonised policies, the EDPS has the opportunity to contribute at that level. Cooperation with supervisory bodies in the third pillar allows him to observe developments in that context and to contribute to a more coherent and consistent framework for the protection of personal data, regardless of the pillar or the specific context involved. This **cooperation** is further dealt with in Chapter 4 of this report.

1.3. Results in 2005

The annual report 2004 mentioned that the following main objectives had been selected for 2005. Most of these objectives have been realised.

— Development of the DPO network

The EDPS has contributed to the development of the network of data protection officers. A position paper on the role of DPOs in ensuring effective compliance with Regulation (EC) No 45/2001 was published in November 2005, and institutions and bodies have been urged to fully benefit from this role.

— Brochures, website and newsletter

The EDPS has ensured a wide circulation of brochures in all official languages, to raise awareness of the rights of data subjects and of his own roles on the basis of the regulation. A newsletter was introduced to provide information about new developments. A completely new website will be launched shortly.

— Notifications and prior checks

All institutions and bodies were invited to notify their existing processing operations, at the latest by spring 2007. The EDPS has invested considerable time and efforts in ‘prior-checking’ processing operations which are likely to present specific risks. Most opinions on prior checks have been published on the website.

— **Guidelines for complaints and inquiries**

The development of standard procedures for complaints, inquiries and other types of cases has taken more time than expected. The main principles will be integrated in the rules of procedure which the EDPS intends to adopt and publish on the website in spring 2006. More detailed guidelines will follow in due course.

— **Audits and investigations**

The EDPS made the necessary preparations for a security audit, about to be held at the central unit of Eurodac, in order to verify compliance with applicable regulations and to develop a methodology which can be applied more widely. The EDPS has also initiated on-the-spot investigations, where this has been necessary for a particular case.

— **Privacy and transparency**

The EDPS issued a background paper entitled ‘Public access to documents and data protection’ in July 2005, with guidelines to encourage good practice in both areas and to help institutions and bodies to decide in cases which require striking a balance between these two fundamental rights.

— **E-monitoring and traffic data**

The EDPS developed a draft paper with guidelines on the processing of traffic and billing data of different kinds of electronic communications (telephone, e-mail, mobile phone, Internet, etc.) in the institutions and bodies, with a view to clarify and enhance the safeguards currently applying to such processing activities. The final version of this paper will be issued in 2006.

— **Opinions on proposals for legislation**

The EDPS issued a policy paper on his role as advisor to the Community institutions on proposals for legislation and related documents. This paper has resulted in a standard practice of formal and informal consultations by the Commission, and systematic follow-up in Parliament and in Council. Six formal opinions on different subjects have been adopted in 2005.

— **Data protection in the third pillar**

The EDPS has given special attention to the development of a general framework for the protection of personal data in the third pillar. A major opinion was issued in December 2005 on the Commission proposal for a draft framework decision on this subject. A number of related issues have been dealt with in other opinions.

— **Development of resources**

Effective management of financial, human and other resources was given much attention in 2005. Consolidation and limited growth of the organisation have enabled the EDPS to gradually develop his roles, in order to address urgent needs for supervision and consultation in most institutions and bodies.

1.4. Objectives for 2006

The following main objectives have been selected for 2006. The results achieved on them will be reported next year.

— **Support of the DPO network**

The EDPS will give strong support to the network of data protection officers, with special emphasis on introduction and coaching of newly appointed DPOs. A timetable will be set for bilateral evaluations of progress in notifications, with a view to notification of existing operations being completed at the latest by spring 2007.

— **Continue prior checking**

The EDPS intends to finalise prior checking of existing processing operations in the fields of health-related data, staff evaluation, disciplinary files, monitoring of communication networks, and social services. A policy paper with an update on relevant practices and conclusions of prior checks will be issued in autumn 2006.

— **E-monitoring and traffic data**

The EDPS will issue a final version of the paper with guidelines on processing of personal data related to the use of electronic communication networks, and will initiate procedures for the case-by-case evaluation and possible approval of data retention lists to be submitted by institutions and bodies.

— **Guidelines for personal files**

The EDPS will develop and issue guidelines on content and conservation periods of personal files on staff in institutions and bodies. These guidelines will be based on conclusions of prior checks and will take due account of staff regulations and data protection requirements.

— **Transfer to third countries**

The EDPS will make an inventory of personal data transfers by the institutions and bodies to third countries, international organisations and European bodies outside the scope of Regulation (EC) No 45/2001 and Directive 95/46/EC, and issue the necessary guidelines, after having heard comments from relevant Community institutions and bodies.

— **Supervision of Eurodac**

The EDPS will conduct an in-depth security audit of Eurodac's central database, and continue to develop close cooperation with national data protection authorities on a system of joint supervision, with a view to build and share experience for other large-scale European databases.

— **Advisory role on legislation**

The EDPS will consolidate and further develop his advisory role on legislative proposals by continuing to issue opinions on various subjects in an effective and timely manner and by seeing his role formally recognised in the legal instruments involved. He will also continue to give adequate follow-up to opinions issued.

— **Interventions in court cases**

The EDPS will consider interventions before the Civil Service Tribunal, the Court of First Instance or the Court of Justice in cases raising issues which are relevant for the interpretation of data protection principles, in order to contribute to a consistent development of data protection law at European level.

— **Second version of website**

A completely revised website will be launched by mid-2006, with online access to the register of prior-checking notifications, opinions and follow-up. The website will be structured according to the main roles of the EDPS and will allow users better access to relevant information on different activities.

— **Development of resources**

The EDPS will continue to develop the necessary resources and infrastructure to ensure an effective accomplishment of his tasks. He will seek a prolongation of the present administrative agreement with the Commission, the Parliament and the Council, and an adequate enlargement of available office space to accommodate current needs and expected increases in staff.

2. SUPERVISION

2.1. General

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

As in 2004, the main aspect of supervision during 2005 was prior checking. This task implies scanning the activities of the institutions and bodies in fields which are more likely to present specific risks for data subjects, as defined in Article 27 of Regulation (EC) No 45/2001. The opinions of the EDPS allow controllers to adapt their processing operations to the guidance of the EDPS, especially where non-compliance with the data protection rules may seriously endanger the rights of individuals. Prior checking is the main tool of supervision, since it allows a systematic approach. The EDPS has other instruments at his disposal such as the handling of complaints.

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

2.2. Data protection officers

The regulation provides that at least one person should be appointed as data protection officer (Article 24.1). Some institutions have coupled the DPO with an assistant or deputy DPO. The Commission has also appointed a ‘data protection coordinator’ in each directorate-general (DG), 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 productive in terms of collaboration and has led to the adoption of certain internal background papers.

The EDPS has attended a part of each of the meetings held between the DPOs themselves in March (EDPS Office, Brussels), July (Court of Auditors, Luxembourg) and October (European Ombudsman, 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 concepts of the regulation relevant in the prior-checking procedure (e.g. controller, processing operations). It also afforded the EDPS the opportunity to outline the progress made in dealing with prior-checking cases and to give details on some of the findings resulting from prior-checking work (see below 2.3.). This collaboration between the EDPS and the DPOs has thus continued to develop in a very positive manner.

The EDPS presented his position paper entitled ‘Public access to documents and data protection’, this being a topic often confronted by DPOs in their work.

Finally, much discussion in the meetings centred on the DPOs' paper 'Profile of DPO and good practice manual' and the EDPS's 'Position paper on the role of the data protection officers in ensuring effective compliance with Regulation (EC) No 45/2001'. These papers were initiated in response to the DPOs' concern about guaranteeing the independence of their function. The DPOs drafted a document which aims at:

- identifying the 'ideal' profile for the DPO in Community institutions or bodies;
- setting some minimum standards as regards their position within the Community institutions or bodies;
- detailing good practices for carrying out their duties and identifying potential criteria for evaluating their work.

This document largely inspired the EDPS's position paper.

In his position paper, sent to the heads of the EU administration, the EDPS underlines the key role of the DPO as a strategic partner in ensuring compliance with the regulation. The EDPS:

- explains how compliance with data protection in the institutions and bodies must be ensured at different levels in which the DPO, the institution or body and the EDPS all have a role to play;
- gives guidance as to how the DPOs can best perform their tasks in an independent manner;
- examines the main functions of the DPOs, which include monitoring of compliance with the regulation, receiving notifications, keeping a register open for public consultation, giving advice and raising data protection awareness within the institution or body itself, and notifying the EDPS of certain processing operations for prior checking.

The key message of the document was not only that also all EU bodies need to appoint a DPO, but that this appointment does not in itself imply automatic compliance with the regulation. DPOs must be notified more adequately of personal data processing within their institution or body and, where appropriate, notify the EDPS of any processing operations which entail specific risks for the people concerned and which therefore need to be prior checked.

2.3. Prior checks

2.3.1. Legal base

General principle: Article 27(1)

Article 27(1) of the regulation provides that all ‘processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of 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 in the list 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 by Article 36, implies specific risks that justify prior checking by the EDPS.

Cases listed in Article 27(2)

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

- (a) *Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures.* These categories are of a sensitive nature and deserve more attention due to the fact that they fall amongst the special categories of data according to Article 10 of the regulation. The EDPS has specified this criterion in the sense that, if the data relating to health or offences, etc. are the result of a processing operation before going into a filing system, it is the previous operation and not the filing system itself that is the object of prior checking. This is the case for personal files in the institutions and bodies. Another distinction to be made is that security measures (*sûreté* in French) are not measures related to security of buildings, for example, but 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.* The criterion is based on the purpose of the processing and not on the mere gathering of evaluation data if there is no purpose of further evaluation of the individual (here too, the previous processing of the evaluation is in itself subject to prior checking).

- (c) *Processing operations allowing linkages, not provided for pursuant to national or Community legislation, between data processed for different purposes.* This provision aims at preventing data collected for different purposes from being linked together. The risk is that it will be possible to deduce new information from the linkage made between the data, not intended for that information, thus diverting the data from the purpose for which they were initially collected. The use of a personal identifier may be a hint, but does not in itself, present a specific risk. The use of electronic databases capable of being searched through by software tools may be another element to be considered.
- (d) *Processing operations for the purpose of excluding individuals from a right, benefit or contract.* This criterion applies typically to debarment systems and may overlap partially with evaluation systems.

2.3.2. Procedure

Notification/consultation

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

Should the DPO have any doubts as to the need for prior checking, he or she may also consult the EDPS on the case (Article 27(3)). This consultation procedure has been a fundamental tool in developing the criteria of interpretation of Article 27(1) and (2), mentioned above. In some cases, the DPO has sent a notification for prior checking assuming that there was a need in the legal sense, but the EDPS concluded that this was not the case (see paragraph 2.3.3, under opinions on prior-checking cases issued in 2005). In any event, those cases, together with consultations, have been of great importance in clarifying the criteria for prior checking.

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 the relevant information.

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.

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 the notification form developed in 2004. In 2005, the prior-check notification form to be filled in by DPOs and sent to the EDPS was improved upon, both in terms of content, by adding some more relevant elements, and in terms of format, allowing an easy interface with internal notification forms sent to DPOs, namely with the format used by the Commission and those other institutions and bodies that follow it.

Experience has demonstrated that more information than foreseen in Article 27(5), by reference to Article 25, is needed to have a good factual and legal basis to analyse processing operations. To that effect, new fields of information have been added to the form. The need to request further information is thus avoided as much as possible.

In the interest of transparency, all information is included in the public register, except the security measures, which are not to be mentioned in the register open for public inspection. This restriction is in line with Article 26 of the regulation, which provides that the register of processing operations held by each DPO shall include the information provided in the notification form, except security measures.

Once the EDPS has delivered his opinion, the reference to the opinion, the case number and possible follow-up measures to be taken (with the same restrictions as mentioned above) are added to the register. Later on, the changes made by the controller in the light of the EDPS opinion are also given in summary form. In this way, two goals are achieved. On the one hand, the information on a given processing operation is kept up to date and, on the other, the transparency principle is complied with.

The register will be available online with the second phase of the website and both the notifications and the opinions issued will then be accessible. Meanwhile, most opinions are posted on the website, including follow-up notes added when recommendations are implemented by the controllers.

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 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.

To guarantee, as in other areas, that the entire team works on the same basis and that the EDPS's opinions are adopted after a complete analysis of all significant information, a case manual is being drafted. It provides a structure of opinions, based on accumulated practical experience and is continuously updated. It also includes a checklist.

A workflow system is in place to make sure that all recommendations in a particular case are followed up and, where applicable, that all enforcement decisions are complied with (see paragraph 2.3.7.)

2.3.3. Quantitative analysis

Distinction of ex post cases and proper prior-checking cases

The regulation came into force on 1 February 2001. Article 50 provides that Community institutions and bodies are to ensure that processing operations already under way on the date the regulation entered into force are brought into conformity with the regulation within one year of that date (i.e. by 1 February 2002). The appointment of the EDPS and the Assistant EDPS entered into effect on 17 January 2004.

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

In order to deal with the backlog of cases likely to be subject to prior checking, the EDPS requested the DPOs to analyse the situation of their institution concerning processing operations within the scope of Article 27. Following the receipt of contributions from all DPOs, a list of cases subject to prior checking was made by the EDPS in 2004. This list was further refined during 2005.

As a result of the inventory, some categories were identified in most institutions and bodies and therefore found suitable for a more systematic supervision. To allow for the most efficient use of the human resources available, the EDPS prioritised the work on *ex post* prior-checking cases. In September 2004, by examining the inventory of cases which have to be submitted by the institutions and bodies to the EDPS, three major priorities were established:

1. medical files,
2. staff appraisal,
3. disciplinary procedures.

The EDPS added two new priorities in the request for an updated inventory to the institutions and bodies in November 2005, namely:

4. social services,
5. e-monitoring.

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

Opinions on prior-checking cases issued in 2005

In 2005, the first complete year of work for the EDPS, **34 opinions** on prior-checking cases were issued.

Court of Auditors	5 prior-checking cases
European Commission	4 prior-checking cases
Committee of Regions	3 prior-checking cases
Council	4 prior-checking cases
European Central Bank	3 prior-checking cases
European Court of Justice	6 prior-checking cases
European Economic and Social Committee	1 prior-checking cases
European Investment Bank	4 prior-checking cases
Parliament	2 prior-checking cases
OHIM ³	2 prior-checking cases

Of the 34 prior-checking cases, only four were proper prior-checking cases, i.e. the institutions and bodies concerned (Court of Auditors for three of them and the ECB for the fourth) followed the procedure involved for prior checking before implementing the processing operation. Three of those four prior-checking cases were related to disciplinary procedures and one to evaluation. The remaining 30 were *ex post* prior-checking cases.

³ Office for Harmonization in the Internal Market (Trade Marks and Designs)

In addition to these 34 prior-checking cases on which an opinion has been issued, the EDPS has also dealt with eight cases which were found to not be subject to prior checking: two notifications came from the Court of Justice, two from the European Investment Bank, two from the European Ombudsman, one from the Committee of the Regions and one from the Commission. Of these eight cases, five dealt with personal files of staff. Although personal files of staff are not subject to prior checking, they exist in all institutions and bodies and raise important data protection issues. This specific subject will therefore be treated in a paper intended to provide guidelines ensuring that the rights of individuals are duly protected.

Analysis by institution/body

Most institutions and bodies have notified processing operations likely to present specific risks. Whilst updating their inventory of prior-checking cases (in November 2005), the institutions and bodies have had the occasion to analyse in which area notifications are progressing well or are missing.

Only one agency (the OHIM) has notified any cases. The EDPS assumes that many other agencies will notify processing operations in the near future, as some of them are already well on their way to determining their own inventories.

Analysis by category

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

Category 1 (medical files)	9 prior-checking cases
Category 2 (staff appraisal)	19 prior-checking cases
Category 3 (disciplinary procedures)	6 prior-checking cases
Category 4 (social services)	none
Category 5 (e-monitoring)	none

Regarding Category 1, it includes the medical file itself (one prior-checking case) and all procedures linked to allowances or sickness schemes (eight prior-checking cases).

The major category theme remains Category 2, relating to the evaluation of staff (56 % of cases; 19 files out of the 34). The appraisal concerns all staff members of the European Community, including officials, temporary agents and contractual agents.

The purpose of evaluation is relevant in a broader sense in that it relates not only to the appraisal itself (for example, Case 2005-218 about the career development review (CDR) system), but also to all processing operations including data which contributed to the evaluation of the data subject in a specific framework (such as the evaluation of the freelance contractors).

Regarding the third category (disciplinary procedures), only six files were dealt with. These processing operations were nevertheless very well documented. It is important to underline that 75 % of the proper prior-checking cases relate to disciplinary procedures.

Since priority themes four and five were only introduced in November 2005, it stands to reason that no opinions have been issued to date, although some notifications have been received in each category.

Work of the EDPS and the institutions and bodies

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

Notifications for prior checking received in 2005, on which opinions are to be issued in 2006

It seems likely that many prior-checking cases will be dealt with during 2006. At the end of January 2006, **33 prior-checking cases** were already in process. Of these, 29 notifications were sent in 2005 (eight in December) and four were notified in January 2006. None of these cases are true prior-checking cases. Only one case has been considered as not subject to prior checking.

European Commission	3 prior-checking cases
Council	8 prior-checking cases
European Central Bank	4 prior-checking cases
European Court of Justice	2 prior-checking cases
European Investment Bank	3 prior-checking cases
EPSO ⁽⁴⁾	3 prior-checking cases
EUMC ⁽⁵⁾	1 prior-checking case
OHIM ⁽⁶⁾	1 prior-checking case
TCEU ⁽⁷⁾	4 prior-checking cases

Analysis by institution and body

The institutions and bodies are continuing to notify to the EDPS, processing operations likely to present specific risks. After having launched the updated inventory (in November 2005), it is noted that numerous notifications were received from some institutions, and relatively few or none were received from others.

In addition to the OHIM, two other agencies (the EUMC and the TCEU) are now active in the area of data protection. More agencies are expected to take on the issue of data protection in the near future.

⁽⁴⁾ European Personnel Selection Office (which relies on the DPO of the Commission).

⁽⁵⁾ European Monitoring Centre on Racism and Xenophobia.

⁽⁶⁾ Office for Harmonization in the Internal Market (Trade Marks and Designs).

⁽⁷⁾ Translation Centre for the Bodies of the European Union.

Analysis by category

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

Category 1 (medical files)	9 prior-checking cases
Category 2 (staff appraisal)	13 prior-checking cases
Category 3 (disciplinary procedures)	1 prior-checking case
Category 4 (social services)	2 prior-checking cases
Category 5 (e-monitoring)	3 prior-checking cases
Other areas	1 prior-checking case ⁽⁸⁾

In Category 1 (medical files) there has been a continuing process of notifications and this is expected to continue in 2006, as many procedures involve medical files.

The Category 2 theme (staff appraisal) still forms the majority of cases — 13 out of 29 files (45 %). Major cases have been notified within this area, such as the recruitment of officials, temporary agents and contractual agents (EPSO cases), which concerns all institutions and bodies.

Regarding Category 3 (disciplinary procedures), the EDPS is expecting notifications from the institutions.

Concerning Category 4 (social services), notifications have already been received (one from the Council and one from the Commission).

Category 5 (e-monitoring) is of particular importance. As a background for the prior checking of e-monitoring systems, a paper about e-monitoring is being drafted by the EDPS and will serve as reference for prior checking in this domain (see paragraph 2.7).

⁽⁸⁾ Related to financial irregularities.

2.3.4. *Main issues in ex post cases*

Medical data and other health-related data are processed by the institutions and bodies. Any data relating to direct or indirect knowledge of the state of health of an individual fall under this category. Therefore, ‘double allocation’ for handicapped children, record of absences, etc. are subject to prior checking.

In this field, both the need for prior checking and the specific conditions relating to the processing of sensitive data apply (Article 10 of the regulation). The legal basis and the strict need for processing those data have been carefully looked into. Confidentiality is another crucial concern.

In some cases, the outsourcing of medical services implies that the processing falls outside the scope of the regulation (but, in those cases, the national legislation transposing Directive 95/46/EC is applicable).

Staff evaluation is a common processing operation in all institutions and bodies, for obvious reasons. A variety of cases have been analysed, from the selection of new personnel to the annual appraisal, affecting both permanent and temporary staff as well as trainees. Apart from the common issues of data retention, information, etc., the purpose limitation has been underlined: no data collected for evaluation can be used for any incompatible use. The conservation of data in personal files is also a relevant issue in these operations. In a particular case of monitoring of telephone calls, traffic data were present in the system and therefore Article 37 was also relevant.

Administrative inquiries and disciplinary proceedings: three cases of *ex post* checking were carried out in this area. As in the proper prior-check cases (see paragraph 2.3.5), the distinction between personal files and disciplinary/administrative inquiry files has been most important in guaranteeing the respect for retention periods. A major problem encountered is that there seems to be a contradiction between the principle of limited conservation of data, plus the principle of prescription of sanctions, and the current interpretation of Article 10(i) of Annex IX to the Staff Regulations. The recommendations of the EDPS and the ongoing work tend to reconcile the data protection principle with the need to take into account the antecedents in cases of new disciplinary misbehaviour.

2.3.5. Main issues in proper prior checks

The EDPS should normally give his opinion prior to the start of a processing operation, so as to guarantee the rights and freedoms of the data subjects from the beginning. This is the rationale of Article 27. In parallel with the handling of *ex post* prior-checking cases, four cases of ‘proper’ ^(°) prior checking were notified to the EDPS in 2005. A general conclusion from all of them is that the information in proper prior-checking cases is frequently not as concrete as concerns the data processing in the *ex post* cases. In proper prior-checking cases, procedural rules are a predominant aspect of the notification.

The ‘Compass case’ of the Court of Auditors dealt with the new evaluation procedure of staff members. The only recommendations to improve the system from a data protection point of view were the inclusion of the information foreseen in Articles 11(1)(f) and 12(1)(f) so as to enhance fairness, the adoption of security measures in communications and the limitation of access to data in the event of an appeal.

The ‘Harassment case’ of the Court of Auditors concerned a system to deal with harassment situations. Initially it was claimed that the ‘informal’ phase of the procedure established by the Court of Auditors was not subject to the regulation since there was no filing of the personal data collected. The EDPS considered that it was of the utmost importance to have this informal phase covered by the regulation, so as to ensure the full application of the guarantees as to the processing of personal data. Given the sensitivity of the issues, recommendations were made in many areas (legal basis, information to data subjects, purpose limitation, etc.).

In the ‘Internal administrative inquiries and disciplinary proceedings case’ of the Court of Auditors, the EDPS *inter alia* gave recommendations as to the processing of sensitive data as defined in Article 10 and to the rights of access and rectification (with specific meaning in this context). The main issue was the distinction of disciplinary files from personal files and the different rules applicable as to the conservation of data.

^(°) I.e. cases concerning processing operations not yet implemented.

The same issues were at stake in the ‘Internal administrative inquiries case’ of the European Central Bank. These inquiries can eventually lead to disciplinary proceedings. There, the possibility of telephone interception was analysed and a restrictive approach was considered admissible. A logical interpretation of the limitation of the conservation of communication traffic data was reached, by interpreting jointly Articles 37 and 20 of the regulation.

2.3.6. Consultations

Should the DPO have any doubts as to the need for prior checking, he or she has to consult the EDPS on the case (Article 27(3)). In 2005, DPOs consulted the EDPS on several subjects.

The EDPS has clarified that the following cases are subject to prior checking:

- e-monitoring of traffic data in the institutions and bodies (Category 5 for the *ex post* prior checks) since it deals with the evaluation of the conduct of individuals;
- systems intended to address the problem of harassment at work, on the same grounds;
- processing operations aimed at professional reorientation of personnel, carried out by a group comprising a doctor, a social assistant, etc.;
- new procedures for promotion.

In other cases, prior checking was not deemed to be necessary:

- screening with a view to granting or not a right, benefit or contract, because Article 27(2)(d) refers only to exclusion (debarment); however, if an evaluation takes place, the case falls under Article 27(2)(b);
- the management of administrative structures, such as job descriptions of staff members, as they do not imply any evaluation and no other risk was present;
- teleworking, unless evaluation mechanisms are introduced in the system.;
- outsourcing the tasks of emergency help teams (since the selection of the team members is the complete responsibility of a private entity).

Medical data processing is a complex area.

- The processing of health-related data by the administrative services of the institution or body is subject to prior checking under Article 27(2)(a).
- When medical services are outsourced to another European institution or body, they are to be prior checked in the latter body and not in the outsourcing one.
- If the services are provided by a private company, the regulation does not apply and the national legislation transposing Directive 95/46/EC is relevant. Therefore there should be no prior checking by the EDPS.
- A borderline case was analysed in which the medical services are provided by a doctor and a nurse in the premises of the institution. As it was concluded that the institution has the role and powers of a controller, prior checking was deemed necessary.
- Health-related data were also the decisive elements to include in the scope of prior checking for a processing operation intended to take due account of disabilities of personnel in case of emergency and to grant them special parking facilities.

From another perspective, to be operative, umbrella systems are not being prior checked in themselves, even if they include sub-systems falling under Article 27. In those cases, the notification of the general system has been used as a background and context information for the checking of the sub-system. A clear example is Sysper 2 of the Commission, which embeds such processing operations as CDR/REC (career development review system of the staff members), obviously subject to prior checking.

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

When the EDPS delivers an opinion on the case submitted to him for prior checking or when a case is analysed to decide on the need for prior checking and some critical aspects appear to deserve correcting measures, the opinion issued by the EPDS may contain a series of recommendations which must be taken into account in order to make the processing operation comply with the regulation. 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 (in paragraphs 2.3.4 and 2.3.5), most recommendations concern information relating to data subjects, data conservation periods, purpose limitation and the rights of access and rectification. Institutions and bodies are willing to follow these recommendations and, to date, there has been no need for executive decisions. The time for implementing those measures varies from case to case. During 2005, six cases have been closed as all recommendations have been implemented ⁽¹⁰⁾. In one case ⁽¹¹⁾, one measure is pending.

As to the follow-up of consultations on the need to prior check in an *ex post* case, if the answer has been positive and the matter is a priority theme (seven cases in 2005), the receipt of the notification is monitored and, if needed, a reminder is sent. In cases where the case falls outside priority matters, the follow-up will consist of the request for a notification in due course. In proper prior-checking cases, the notification is requested immediately. In the remaining cases, specific risks in the sense of Article 27 were not found to be present but, nevertheless, some aspects had to be changed; one has been closed, as those changes were made, and the other two are still pending.

⁽¹⁰⁾ Council of the European Union: 2004/319. European Parliament: 2004/13 and 2004/126. European Commission: 2004/95 and 2004/96. OHIM: 2004/174.

⁽¹¹⁾ European Commission — 2004/196.

2.3.8. Conclusions and future

The year 2005 saw intense activity in the domain of prior checking. The results are quite satisfactory, although several institutions and bodies have not sent notifications in the priority matters of *ex post* checking. The year 2006 must be the decisive year to obtain this information and to complete the analysis of the processing operations in all institutions and bodies in those fields. This process should be finalised no later than spring 2007. The EDPS will make all efforts to achieve that goal. New bodies, as well as institutions in existence for a longer period, must revise their personal data-processing operations in all fields, but especially in the priority matters, to make sure they comply with that deadline.

Electronic communications will receive specific attention during 2006. The EDPS is preparing a paper on the subject (see paragraph 2.7). As the e-monitoring for traffic and budgetary purposes, including the verification of authorised use, as decided by each institution and body, is subject to prior checking under Article 27(2)(b), DPOs are expected to send the relevant notifications of existing systems as soon as the EDPS has issued his paper on the subject. This includes the list referred to in Article 37(2).

Awareness of the possible need for prior checking in the phase of design of new systems also needs to be raised. The implementation timetable of new projects has to take account of the period necessary for the institution or body to allow the DPO to notify the EDPS, and for the EDPS to issue his opinion, in order to be in a position to implement the EDPS recommendations before launching the processing operation.

As to the procedure, shorter deadlines for informing the EDPS, when further information is requested, are desirable. In fact, the complete filling out of notification forms and exhaustive back-up documents should make the further information request the exception rather than the rule, as it has been until now.

Support for newly appointed DPOs and a timetable of bilateral revisions of the notification process with all DPOs, with a view to accomplishing the above objectives, should be developed. A policy paper with an update on the practices and conclusions of prior checking will be an important tool in that context.

2.4. Complaints

2.4.1. Introduction

In accordance with Articles 32(2), 33 and 46(a) of the regulation, any natural person may lodge a complaint to the EDPS, with no conditions of nationality or place of residence ⁽¹²⁾. Complaints are only admissible if they emanate from a natural person and concern the breach of the regulation by an EU institution or body when processing personal data in the exercise of activities all or part of which fall within the scope of Community law. As we will see below, a number of complaints filed to the EDPS were declared inadmissible by reason of the EDPS not being competent.

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

If the case is admissible, the EDPS will proceed to inquire about the case, notably by contacting the institution or body concerned or by requesting further information from the complainant. The EDPS has the power to obtain from the controller or the institution or body access to all personal data and to all information necessary for the enquiry and obtain access to any premises in which a controller or institution or body carries out its activities.

The EDPS received 27 complaints in 2005. Of these cases, only five were declared admissible and further examined by the EDPS. Furthermore, four decisions were adopted by the EDPS concerning complaints introduced in 2004. These will also be briefly examined below.

⁽¹²⁾ According to Article 32 (2): '[...] every data subject may lodge a complaint to the European Data Protection Supervisor 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 European Data Protection Supervisor regarding an alleged breach of the provisions of [Regulation (EC) No 45/2001], without acting through official channels'.

Article 46 (a) European Data Protection Supervisor shall 'hear and investigate complaints, and inform the data subject of the outcome within a reasonable period'.

2.4.2. Cases declared admissible

Pending 2004 cases

As mentioned above, for some cases, although filed in 2004, the EDPS took his decision in 2005.

One complaint received in 2004 (2004-111) concerned the disclosure of personal data of persons involved in a competition case. The Commission can decide about the (non-)confidentiality of some personal data collected in competition cases. The complainant challenged the decision made concerning her. Although the complainant raised interesting questions, she did not provide the EDPS with the information needed to pursue the case. The EDPS was therefore not able to issue a decision.

Another complaint pending from 2004 (2004-329) concerned the collection of data needed for the reimbursement of travel expenses for an expert who participated in a meeting organised by the European Commission (Article 4 of the regulation: data quality). The EDPS made a request to the Commission and as a result found the collection of personal data relevant, adequate and not excessive.

Finally, a complaint received in 2004 (2004-7) concerned illegal access and disclosure of information contained in Sysper 2 (information system of the European Commission) in breach of Article 21 of the regulation (security). After exchanges of information on this case, the Commission informed the EDPS that an IDOC inquiry will be opened.

Cases for 2005

A complaint was made against the European Parliament for the publication of the names of petitioners (2005-40). It was questioned whether the processing was lawful (Article 5) and whether the level of information provided was sufficient, in order for consent to be a valid ground for processing/disclosure (Article 2). The main findings were that the processing was lawful, not on the grounds of unambiguous consent, but on the grounds of Article 5(a) and (b) — ‘tasks carried out in the public interest’ and ‘legal obligation’, respectively. The information given to the data subjects

was, however, not sufficient and the EDPS therefore suggested that the Secretariat of the Committee on Petitions amend the forms for filing a petition, so that the consequences were made more visible. The EDPS also suggested that the possibility to opt-out from disclosure on compelling and legitimate grounds be introduced.

A complaint was made against the European Commission regarding a ‘profile’ of the person online (2005-112). One of the participants at a three-day conference organised by the European Commission wanted to delete his profile, provided before the conference, from its publication on a specific section of the Europa website. The data subject contacted the EDPS to object (Article 18) to the disclosure of his résumé. The EDPS forwarded the request to the official in charge of the particular website, asking him to look at the merits of the case. The official subsequently chose to delete the profile.

A complaint was received concerning the right of access (Article 13) to personal data concerning internal selection competition at OHIM (2005-144). This complaint raised interesting questions on the right of access in the selection procedures as organised by EPSO. It triggered an on the spot investigation by the EDPS. Following this investigation, the EDPS considered that access to data should be given. This was subsequently granted to the complainant.

Another complaint was made against a selection procedure in the European Parliament (2005-182). The complainant (candidate for a post) asked for rectification of his personal data in the database of the European Parliament (Article 14). The EDPS decided that information on the right of access and rectification concerning certain databases must be provided to staff. However, concerning the actual rectification of data, the EDPS held that he can only act concerning factual data, but that he has no competence relating to evaluation data.

A complaint was made by a journalist who claimed the — non explicit — disclosure of his name in a case of bribery by an OLAF press release (2005-190). His claims were made on the basis of fair processing (Article 4) and right of rectification (Article 14). The complainant had already submitted a complaint to the Ombudsman. The EDPS closed the case as he could not add anything to the Ombudsman’s findings in this case.

A complaint was submitted to the EDPS (2005-377) concerning certain information published in the press, concerning a disciplinary procedure against two EU officials. The aim of the complaint was to establish how this information could have been made known outside the European Commission. The EDPS has decided not to open any investigation, due to lack of sufficient evidence.

2.4.3. Cases not declared admissible: main reasons for inadmissibility

Out of the 27 complaints received in 2005, 22 were declared not admissible for reason of lack of competence of the EDPS. Indeed, the cases did not concern processing of personal data by the European institutions and bodies, and so should have been referred to national data protection authorities. In one case, the complaint concerned information on the website of the Council of Europe, which does not qualify as a Community institution/body. The EDPS referred the complainant to the Council of Europe.

2.4.4. Collaboration with the Ombudsman

According to Article 195 of the EC Treaty, the Ombudsman is empowered to receive complaints concerning instances of maladministration in the activities of the Community institutions or bodies. The European Ombudsman and the EDPS have overlapping competences in the area of complaint handling in the sense that instances of maladministration may concern the processing of personal data. Therefore, complaints brought before 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 to a maximum extent a consistent approach to both general and specific data protection issues raised by complaints, an exchange of information takes place between the two institutions concerning both the introduction of complaints which are of relevance for the other institution and about the outcome of the complaint itself.

Further work is being carried out examining the different forms of possible collaboration between the European Ombudsman and the EDPS, aiming at a more structured collaboration in the near future.

2.4.5. Further work in the field of complaints

The EDPS has been working on the drafting of an internal case manual for complaint handling by EDPS staff.

Two members of staff also attended the complaint handling workshop for national data protection authorities in Paris in November 2005. During this two-day workshop, EDPS staff presented an overview of the complaints handled by the EDPS and elements of the communication strategy. The workshop was an interesting occasion to share experience in this field and to learn from complaint handling at a national level.

2.5. Investigations

The Assistant Supervisor and a member of his team carried out the first on-the-spot investigation by the EDPS under Article 47 of the regulation in the context of a complaint regarding the right of access to data. The data concerned results of an oral exam in an internal selection procedure within an EU agency. The visit enabled the EDPS to determine the exact scope of the data, access was being requested to. The visit was also used to meet different services of the institution and to explain the main functions and activities of the EDPS.

2.6. Public access to documents and data protection

As announced in the annual report for 2004, the EDPS invested considerable efforts in the elaboration of a background paper which deals with the relationship between the regulation and the public access regulation ⁽¹³⁾ and which was presented in July. Both fundamental rights, neither prevailing over the other, are essential elements of democratic life in the European Union. They also form an important part of the notion of good governance. Many documents held by EU

⁽¹³⁾ Regulation (EC) No 1049/2001.

institutions and bodies contain personal data. For these reasons, an appropriate and well-thought-through approach to the possible disclosure of a public document containing personal data is of high importance.

The paper contains a description as well as an analysis of the relationship between the two fundamental rights and provides practical examples and a checklist so as to guide the responsible officials and services of the EU administration. The paper was generally well received and has been used in the daily work in some of the institutions and bodies.

The bottom line of the paper is that there can be no automatic refusal to documents held by the EU administration just because they contain personal data. The ‘Article 4(1)(b) exception’⁽¹⁴⁾ of the public access regulation stipulates that the privacy of a person needs to be undermined for disclosure to be hindered. Urging for a concrete and individual examination in each case, the paper puts the carefully worded exception into context by arguing that the following criteria must be met for the non-disclosure of a public document:

1. the privacy of the data subject must be at stake;
2. public access must substantially affect the data subject;
3. public access is not allowed by the data protection legislation.

The paper interprets the third criterion as follows. On a case-by-case basis, it has to be assessed whether disclosure of a document that relates to the privacy of someone is in compliance with Articles 4, 5 and 10 of the data protection regulation. If disclosure is in line with the principles relating to data quality and to lawful processing, it is, according to the EDPS proportionate to make the document public, as long as it does not contain sensitive data.

The paper finally, lays down two important notions that have to be taken into account.

1. People acting in a public capacity will be subject to a higher degree of public interest. This context can require that their personal data may be disclosed.
2. A proactive approach is always advisable. This means that the institution or body concerned informs the data subject about its transparency obligations and that certain personal data, by analogy, may be made public.

⁽¹⁴⁾ ‘The institutions shall refuse access to a document where disclosure would undermine the protection of [...] privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.’

2.7. E-monitoring

The use of electronic communication tools within the institutions and bodies increasingly generates personal data, the processing of which triggers the application of the regulation. At the end of 2004, the EDPS started work on the processing of data generated by the use of electronic communications (telephone, e-mail, mobile phone, Internet, etc.) in the European institutions and bodies. This project was partially based on background information provided by the DPOs on the practices of their institution in this field. It was also been inspired by findings made during the examination of cases submitted to the EDPS for prior checking. A draft paper has been submitted to the DPOs and should lead to further debates with stakeholders before final publication in June 2006.

2.8. Eurodac

In January 2004, the former joint supervisory authority of Eurodac was replaced by the EDPS, pursuant to Article 20(11) of the Eurodac regulation ⁽¹⁵⁾. Since then, the EDPS has been in charge of the supervision of Eurodac's Central Unit. However, an essential aspect of the supervision of Eurodac as a whole is the cooperation between national supervisory authorities and the EDPS to examine implementation problems in connection with the operation of Eurodac, to examine possible difficulties during checks by the national supervisory authorities and to draw up recommendations for common solutions to existing problems.

Supervision of the Central Unit

As the supervisory authority of the Central Unit, the EDPS has launched a comprehensive inspection in two steps:

- a first inspection of the Central Unit premises and of the network infrastructure, which resulted in a final report early in 2006;
- an in-depth security audit of the Central Unit's databases and its premises in order to evaluate whether the security measures implemented comply with the requirements defined by the Eurodac regulation (to be realised in the course of 2006).

⁽¹⁵⁾ 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.

The first inspection consisted of visits to the Eurodac premises in May 2005, a thorough study of the documentation relating to the functioning of Eurodac, and several meetings with the various officials in charge of the security and the running of the system. These initial activities resulted in a detailed questionnaire which has been communicated to the Commission. This questionnaire addresses issues regarding risks and incident management, documentation on security, physical and logical access control, security of communications, information security education and training, statistics, direct access and direct transmission of data from Member States. On the basis of the analysis of the answers to the questionnaire and of the assessment made during the visits, a draft report was prepared and sent to the Commission in December 2005. A final report was adopted in February 2006 taking into account the comments made by the Commission.

In parallel, the EDPS undertook the necessary step to organise a fully fledged security audit of the Central Unit. For this purpose, an agreement has been made with the recently created European Network and Information Security Agency (ENISA) with a view to assist the EDPS in the performance of the audit.

Cooperation with national data protection authorities

In his annual report 2004, the EDPS presented a vision relating to the supervision of Eurodac ⁽¹⁶⁾. As a result, the EDPS also developed his role in providing a platform for cooperation in supervision and exchange of experiences with the national DPAs. Taking into account the relevant regulatory framework as well as the annual reports published by the Commission on the functioning of Eurodac ⁽¹⁷⁾, a list of topics has been elaborated for discussion in a meeting with DPAs and a possible follow-up at national level on the basis of a joint methodology. This approach has proven very useful in the context of the supervision of other large-scale information systems, such as the Schengen information system.

⁽¹⁶⁾ Annual report 2004, page 34: ‘The EDPS is the supervisory authority for Eurodac’s Central Unit, and also monitors the lawfulness of the transmission of personal data to the Member States by the Central Unit. The competent authorities in the Member States, in turn, monitor the lawfulness of the processing of personal data by the Member State in question, including their transmission to the Central Unit. This means that the supervision must be exercised at both levels, in close cooperation.’

⁽¹⁷⁾ The second annual report was published on 20 June 2005, with reference SEC(2005) 839.

A first coordination meeting with national DPAs was held on 28 September 2005. It prompted a very welcome exchange of information and was a useful occasion to discuss a common approach for supervision. The participants selected, from a list prepared by the EDPS, a short series of topics which should benefit from further scrutiny and agreed on three main issues: special searches, possible use of Eurodac for other purposes than those foreseen in the Eurodac regulation, and the technical quality of data. These issues would be investigated at national level, and the results of the investigation will be compiled by the EDPS and then discussed during a second meeting in late spring 2006. The EDPS looks forward to the results of this first coordinated approach.

3. CONSULTATION

3.1. Introduction

This first complete year in which the European Data Protection Supervisor (EDPS) fully exercised his consultative powers was important for two reasons. Firstly, the EDPS developed a policy on his role as an advisor to the Community Institutions on proposals for legislation (and related documents). Secondly, the EDPS submitted opinions on a number of substantial proposals for legislation.

The policy of the EDPS was laid down in a policy paper in which he describes the ambition to become an authoritative advisor with a wide mandate that includes all matters concerning the processing of personal data. This wide interpretation of his mandate results from the mission formulated in Article 41 of Regulation (EC) No 45/2001 and was confirmed by the Court of Justice. The Court has emphasised that the advisory task does not only cover the processing of personal data by the EU institutions or organs ⁽¹⁸⁾. It also includes legislative proposals in the third pillar of the EU Treaty (police and judicial cooperation in criminal matters).

⁽¹⁸⁾ Orders of 17 March 2005 in two cases concerning the processing of the 'PNR-data' (see paragraph 3.4.2).

Substantial proposals were presented by the Commission in 2005, implementing the Hague programme, approved by the European Council in November 2004. This programme strengthened the priority of action at EU level in the area of freedom, security and justice with an emphasis on law enforcement, including opening up the possibilities for an increase in the exchange of data between authorities of the Member States. In this context, the programme recognised the need for adequate rules for the protection of personal data. The most important developments relating to data protection were those indicated below.

- A third central piece of legislation on data protection at the European level was prepared: the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters aims to provide for protection in an area where many sensitive data are processed and where the level of protection provided for at the European level can be seen as insufficient for seeing that Directive 95/46/EC does not apply.
- The legislative proposals on the second generation Schengen information system (SIS II) and on the visa information system (VIS) have contributed to the further development of large-scale information systems. For example, the VIS is designed to process 20 million entries a year regarding people who apply for a Schengen visa.
- For the first time, private parties will be obliged by EU legislation to retain personal data and thus to install databases for the sole purpose of combating serious crime. This obligation is the consequence of the directive on data retention.

The EDPS exercises his consultative mandate not only by issuing opinions on legislative proposals but also by several other means. The EDPS intervened for the first time in cases before the Court of Justice, in particular in the ‘PNR cases’, and has brought forward his points of view on important matters of data protection before the Court. Moreover, the EDPS has expressed his points of view on several occasions, such as public conferences and seminars and in meetings of the LIBE Committee of the European Parliament.

Finally, the mandate of the EDPS as a consultative body is not strictly related to legislative proposals. Article 28(1) of the regulation confers a mandate in relation to administrative measures relating to the processing of personal data involving one or more Community institutions or bodies. Article 46(d) specifies this mandate as far as implementing rules are concerned.

This chapter of the annual report will not only give an overview of the main activities of 2005 and — as far as possible — their effect, but will also look ahead to the challenges for the coming years. These include examining the consequences of new technological developments as well as of new developments in the field of policy and legislation.

3.2. The policy of the EDPS

Policy paper 'The EDPS as an advisor to the Community institutions on proposals for legislation and related documents' (March 2005)

This policy paper aimed at positioning the EDPS as an authoritative, reliable and consistent advisor to the Commission, the European Parliament and the Council in the process of legislation. In other words, the EDPS envisages becoming a self-evident partner in this process. The three basic elements of his consultative role are clarified in this paper.

The first element includes the scope of his role: the issues on which consultation of the EDPS is required. As said before, the scope is wide, since proposals on many subject matters can affect the protection of personal data.

The second element relates to the substance of the interventions. Interventions by the EDPS are based on the general notion that contributions to the legislative process should not only be critical but also constructive.

- It is crucial to make the relevance of a proposal to the protection of personal data visible.
- Article 6 of the EU Treaty calls for ensuring the respect of fundamental rights as guaranteed by the ECHR, in particular by the case-law on Article 8 of the European Charter on Human Rights. Legal instruments should not deprive a private person from the core of the protection that he or she is entitled to.
- The EDPS will not only act as a privacy watchdog but will take into account that good governance also requires the respect of other justified public interests.
- Proposals should not be merely rejected, but the EDPS will provide alternatives.

The third element relates to the role the EDPS envisages playing within the institutional framework. In order to be effective as an advisor to the three central players in the process of legislation, timing of the interventions is of utmost importance. The policy paper foresees different moments of intervention. Before the Commission proposal is adopted, an informal consultation can take place by the responsible service of the Commission. It has become practice that this informal consultation happens in parallel with the internal inter-service consultation in the Commission. Subsequently, the formal and public consultation takes place on the basis of the Commission proposal. The EDPS endeavours to present his opinions at an early stage of the proceedings within the European Parliament and the Council. A third, optional step of intervention has become standing practice in the more important dossiers: a further informal consultation by the European Parliament and by the Council. The EDPS has not only on several occasions presented his formal opinion orally within the LIBE Committee of the European Parliament and the competent working groups of the Council, but has also at a later stage — quite often at the request of one of those institutions — been available for further consultation.

Finally, the role of the EDPS overlaps to a large extent the advisory functions of the Article 29 Working Party. The policy paper emphasises that they should not act as competitors. In practice, they assume a complementary role, in the interest of the protection of personal data. The fact that two bodies present their opinion on important proposals only strengthens the importance given to data protection in the legislative process, provided, of course, that the messages given by those two bodies do not contradict each other. A contradiction has not yet taken place and is not expected to take place, not only because the EDPS is a member of the Article 29 Working Party but also because both bodies defend the same substantial interests.

When a proposal is based on Title VI of the Treaty of the European Union (the third pillar), in which case the Article 29 Working Party has no formal advisory role, there is an overlap with opinions of other — informal — groups of national data protection authorities. The EDPS has taken a practical cooperative approach that works satisfactorily.

Implementation of the policy paper

Several subjects in the area of freedom, security and justice, were central to the activities of the EDPS during 2005. The following principles have been taken into account by the EDPS.

- The elaboration of the principle of proportionality, to examine whether or not a proposal strikes the right balance between the need for adequate law enforcement and the protection of personal data.
- The elaboration of issues related to large-scale information systems such as the VIS and SIS II, in particular on the security of these systems and on the access to these systems.
- Support for an important step for data protection that has been set by the proposal for a Council framework decision on data protection in the third pillar.
- Within the Commission, the Justice, Freedom and Security DG has increasingly become the natural counterpart of the EDPS: it is responsible for fundamental rights, coordinates data protection within the Commission and deals with most of the important dossiers. In its communication of 10 May 2005 on the Hague programme, the Commission has described 10 priorities in the work of the Justice, Freedom and Security DG. The Commission emphasises the balancing of the principle of availability — central to the Commission's approach — with the protection of fundamental rights.
- The second directorate-general that deals with dossiers of high relevance for data protection is the Information Society and Media DG. In 2005, the issues dealt with by the Information Society and Media DG did not represent an important part of the consultative work of the EDPS, but this is expected to change in 2006.

On the procedural level, the EDPS has established a working method. He has based his priorities on the work programme of the Commission for 2005, as well as other relevant planning tools of the institutions. A few dossiers have been added on the initiative of the EDPS. The dossiers are classified either as 'high priority' requiring an early proactive involvement of the EDPS, and in any case his formal opinion, or as 'low priority' not requiring a proactive involvement (and not necessarily leading to a formal opinion).

The EDPS envisages establishing his priorities in the same way for the coming years and to inform the Commission about his initial conclusions.

3.3. Legislative proposals

3.3.1. *The opinions of the EDPS in 2005* ⁽¹⁹⁾

Opinion of 13 January 2005 on the proposal for a Council decision on the exchange of information from criminal records

This proposal by the Commission was introduced as a measure with a limited time horizon which is intended to cover an urgent lack in the provision for the exchange of information from criminal records, until a more definitive legal instrument is developed. The need for the proposal was triggered by the Fourniret case, a case that raised much public attention and which concerned a French national who had moved to Belgium. Information on his earlier convictions related to paedophilia was not known to the Belgian authorities. The proposal contains two new provisions on the exchange of information on convictions.

The relatively short opinion of the EDPS must be seen in the light of the urgency and the temporary character of the measure. The EDPS advised limiting the proposal to the exchange of information on convictions for certain serious crimes. He furthermore suggested specifying the safeguards of the data subject.

Opinion of 23 March 2005 on the proposal for a regulation of the European Parliament and of the Council concerning the visa information system (VIS) and the exchange of data between Member States on short-stay visas

This Commission proposal aims at improving the administration of the common visa policy by facilitating the exchange of data between Member States. The VIS will be based on a centralised architecture comprising a database where the visa application files will be stored: the central visa information system (CS-VIS) and a national interface (NI-VIS) located in the Member States. The regulation envisages introducing biometric data (photograph and fingerprints) during the application procedure, and storing them in the central database. The VIS will contain (and allow exchange of) biometric data on an unprecedented scale (20 million entries on visa applications a year) reaching a potential 100 million entries after the maximum retention period of five years.

⁽¹⁹⁾ See Annex F.

The EDPS recognises that the further development of a common visa policy requires an efficient exchange of relevant data. One of the mechanisms that can ensure a smooth flow of information is the VIS. However, such a new instrument should be limited to the collection and exchange of data, as far as such a collection or exchange is necessary for the development of a common visa policy and is proportionate to this goal. In particular, routine access by law enforcement authorities would not be in accordance with this purpose.

Regarding the use of biometrics in the VIS, the EDPS recognises the advantages of this use, but stresses the major impact of the use of such data and suggests the insertion of stringent safeguards for their use. Moreover, the technical imperfection of fingerprints requires that fallback procedures are developed and included in the proposal, in order to avoid unacceptable consequences for a great number of people.

Concerning visa checks at external borders, the EDPS took the view that a sole access to the protected microchip by the competent authorities for carrying out checks on visas is sufficient, and avoids access to the central database.

Opinion of 15 June 2005 on the proposal for a Council decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of advance passenger information (API) / passenger name record (PNR) data

This agreement with Canada is the second in a series of agreements with third countries on these matters. The first agreement with the United States of America has been contested before the Court of Justice by the European Parliament and the EDPS has supported the conclusions of the Parliament (see paragraph 3.4.2). The EDPS focused this opinion on the essential differences between the agreement with Canada and the agreement with the USA.

- The proposal foresees a ‘push’ system, which enables the airlines in the European Community to control the transfer of data to the Canadian authorities, contrary to the ‘pull’ system.
- The commitments by the Canadian authorities are binding.
- The list of PNR-data to be transferred is more limited and excludes the transfer of sensitive information.
- The legislative system of data protection in Canada is much more developed than that of the USA.

The EDPS approved of the main substantive elements of the proposal. However, he concluded that the agreement entails an amendment of Directive 95/46/EC and that for this reason the assent of the European Parliament should have been obtained before concluding the agreement.

Opinion of 26 September 2005 on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC

This proposal was issued in the context of growing concerns about terrorist attacks and was closely linked to the combating of terrorism (and other serious crime), in the aftermath of the London bombings of July 2005.

According to the EDPS, the proposal is of significant importance.

- For the first time, an instrument of European law obliges private parties to retain data for the purpose of enforcement of criminal law. The point of departure is contrary to the existing obligations under EC law, since it is laid down that providers of telecommunications services are only allowed to collect and store traffic data for reasons directly related to the communication itself, including billing purposes. Data must be erased afterwards (subject to exceptions).
- It is an obligation that directly concerns all EU citizens.

The EDPS is aware that an adequate availability of certain traffic and location data can be a crucial instrument for law enforcement agencies and can contribute to the physical security of persons. However, in the opinion, the EDPS mentioned that this does not automatically imply the necessity of the new instruments, as foreseen in the present proposal. According to the EDPS, the necessity of this new obligation to retain data — in its full extent — had not been adequately demonstrated.

Nevertheless, recognising that the adoption of a legal instrument on data retention might well happen anyway, the EDPS focused the opinion on the proportionality of the proposed measures. He emphasised that retention of traffic and location data alone is in itself not an adequate or effective response. Additional measures are needed, so as to ensure that the authorities have targeted and quick access to the data needed in a specific case. Furthermore, the proposal should limit the retention periods, limit the number of data to be stored and contain adequate safety measures.

The EDPS asked for the following modifications to the proposal:

- specific provisions on access to the traffic and location data by the competent authorities and on the further use of the data,
- additional safeguards for data protection and further incentives for the providers to invest in an adequate technical infrastructure, including financial compensation of additional costs.

Finally, the EDPS strongly opposed the legal argument that a first pillar proposal could not include rules on access by police and judicial authorities.

Opinion of 19 October 2005 on the proposals regarding the second generation Schengen information system (SIS II)

The Schengen information system (SIS) is an EU large-scale IT system which was created in 1995 as a compensatory measure following the abolition of internal border controls within the Schengen area. A new second generation Schengen information system (SIS II) will replace the current system, so allowing the enlargement of the Schengen area to include the new EU Member States. It will also introduce new characteristics such as: widened access to the SIS (by Europol, Eurojust, national prosecutors and vehicle licensing authorities), interlinking of alerts, and the addition of new categories of data, including biometric data (fingerprints and photographs). The Schengen provisions elaborated in an intergovernmental framework will be fully transformed in instruments of European Union law, which the EDPS welcomes.

The proposals for establishing the SIS II mainly consist of a proposed regulation which will govern the first pillar (immigration) aspects of the SIS II and a proposed decision which will govern the use of SIS for third pillar purposes ⁽²⁰⁾. The EU Treaty makes it necessary to regulate this single system using two main instruments. The result, however, is extremely complex and this required a careful study of the entire legal environment. The EDPS underlined that the new legal regime, however complex, should ensure a high level of data protection, be predictable for citizens as well as for authorities sharing data, and be consistent in its application to different (first or third pillar) contexts.

⁽²⁰⁾ There is even a third proposal: a proposed regulation based on Title V (Transport) regarding specifically the access to the SIS data by authorities in charge of vehicle registration.

The EDPS identified several positive points which represent an improvement compared to the present situation, but also some reasons for concern: the addition of new elements in SIS II, increasing its possible impact on the lives of the individuals, should be met by more stringent safeguards which are described in the opinion; in particular those listed below.

- Access to SIS II data cannot be given to new authorities without the strongest justification. It should also be restricted as much as possible, both in terms of accessible data and authorised persons.
- Interlinking of alerts may never lead, even indirectly, to a change in access rights.
- The impact of the insertion of biometric data does not seem to be sufficiently thought through, and the reliability of these data seems overstated. However, the EDPS recognises that the insertion of these data can improve the performance of the system and help the victims of identity theft.
- Supervision of the system must be ensured in a consistent and comprehensive way at both European and national levels.

Opinion of 19 December 2005 on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

This Commission proposal aims at setting common standards for data protection in the third pillar, an area currently governed by non-harmonised national legislation. This timely proposal will be as important as the data protection directive (95/46/EC) and the Council of Europe Convention 108. In his opinion, the EDPS welcomed the proposal, aimed at ensuring that the fundamental right to personal data protection is guaranteed also with regard to the increasing exchanges of personal data between law enforcement and judicial authorities of EU Member States.

An effective protection of personal data is not only important for the data subjects but also contributes to the success of the police and judicial cooperation itself. The EDPS stressed the importance of ensuring consistency with the current data protection legislation (in particular, Directive 95/46/EC and Convention 108), while providing an additional set of rules addressing the specific nature of law enforcement. It is essential that the main data protection rules cover all police and judicial data — not only data exchanged between Member States, but also data used within one country.

According to the EDPS, personal data should be collected and processed for specified and explicit purposes (a specific offence, a specific investigation, etc.), while further use might be allowed under very strict conditions. Furthermore, it is imperative that: data on different categories of persons — suspects, convicted persons, victims, witnesses, contacts — are processed with different, appropriate conditions and safeguards; specific provisions on automated individual decisions are introduced; and exchanges of personal data with third countries are adequately protected.

3.3.2. Horizontal themes

The necessity to prevent crime and face terrorist threats, as well as the progressive development of the internal and external aspects of the area of freedom, security and justice, have marked the path of the EU institutions working programme, and, consequently, the EDPS agenda. Therefore, in 2005 the EDPS operated in a more complex legal and institutional environment, embracing a wide range of initiatives concerning not only policies related to the free movement of persons (falling under the ‘first pillar’) but also provisions on police and judicial cooperation in criminal matters (third pillar).

The EDPS welcomes that his consultative role on third-pillar legislative proposals has been reflected in the Commission’s practice of carrying out both informal and formal consultations on its proposals relating to the third pillar. It is hoped that the next step will be that consultation of the EDPS (in the first and third pillars) will be made even more visible to the outside world, by mentioning the consultation of the EDPS in the preamble of proposals.

The pillar structure of the EU Treaty has raised new issues and challenges, stemming not only from the different actors taking part in the decision-making process, but also from possible overlapping and interferences between different legal bases and legislative proposals. Clear examples can be found in many EDPS opinions adopted in 2005. In the two opinions on PNR for Canada and the retention of telecommunications data, the EDPS analysed the safeguards and conditions to be followed when personal data collected for commercial purposes are used for the purpose of crime prevention. In the opinion on data retention, the EDPS had to consider different parallel proposals and express his opinion on the most appropriate legal basis, while the opinion on SIS II dealt with a package of legal instruments addressing both first and third pillar aspects of the proposed system.

In this context, the EDPS has endeavoured to ensure, to the maximum possible extent, the consistency of data protection rules throughout all EU legislation, in spite of the pillar structure and the differences in decision-making procedures and institutional actors. This approach explains the warm welcome expressed by the EDPS in his opinion on the Commission proposal for a framework decision on data protection, aimed at setting common EU data protection standards in police and judicial cooperation.

Following his policy paper, the EDPS has used proportionality as one of the main guiding principles of his opinions on legislative proposals: processing of personal data shall be allowed only insofar as it is necessary and provided that no other less privacy intrusive means would be equally effective. This assessment has been carried out from a wider perspective, taking into account all the different, sometimes contradictory, public interests at stake. Where possible, the EDPS has followed a proactive approach by proposing viable alternative solutions that could address law enforcement needs while better preserving the fundamental right to the protection of personal data. In his opinion on the framework decision on data protection in third pillar, the EDPS has highlighted how in some cases good data protection can serve the needs of both data subjects and police and judicial authorities.

With regard to the timing of his interventions, the EDPS has in all cases delivered his opinions at an early stage of the decision-making process, so as to allow both citizens and relevant institutional actors to properly take into account his views. Furthermore, the EDPS has increasingly availed himself of the possibility to give his informal opinion before a Commission proposal is adopted.

3.4. Other activities in the area of consultation

3.4.1. Related documents

In 2005, the EDPS also dedicated more attention to documents preceding formal proposals, such as Commission communications. These kinds of documents often serve as the basis for policy choices made in proposals for legislation, and the EDPS considers the possibility to react to them as an important occasion to express his views on the long-term aspects of data protection policies.

This has been the case with the Commission communication on the external dimension of the area of freedom, security and justice. This communication identifies a strategy in the external dimension of justice, freedom and security policies. The EDPS supported the view that external and internal aspects are intrinsically linked, and encouraged the Commission to take a proactive role in promoting the protection of personal data at an international level, by supporting bilateral and multilateral approaches with third countries and cooperation with other international organisations.

3.4.2. Interventions before the Court of Justice

In 2005, the Court of Justice allowed the EDPS to intervene, for the first time, in two cases before the Court. In these cases, the European Parliament sought the annulment of a Council decision on the conclusion of an agreement between the EC and the USA on the processing and transfer of PNR data by air carriers to the United States. The Parliament also sought to annul the Commission decision on the adequate protection of personal data contained in the PNR of air passengers transferred to the USA.

The EDPS intervened in support of the conclusions of the European Parliament and presented written submissions to the Court. The points of view of the EDPS were defended orally during the Court hearing. The essential points were:

- the decisions do not allow the European airlines to respect their obligations under Directive 95/46/EC and therefore modify the obligations under the directive (since an agreement with a third country has precedence over internal EU law);
- the decisions violate the protection of fundamental rights;
- the Commission exceeds its margin of appreciation under Article 25 of the directive.

On 22 November 2005, the Advocate-General presented his opinion in which he proposes to annul the decisions; however, with a completely different reasoning to the one defended by the EDPS.

3.4.3. Administrative measures

In 2005, the EDPS exercised his consultative powers on administrative measures and more in particular on implementing rules of institutions and bodies in the area of data protection in the following ways.

The EDPS has developed an approach on the specific implementing rules concerning the DPOs as foreseen in Article 24(8) of the regulation. According to the EDPS, the scope of the implementing rules should be as broad as possible, to include aspects that directly affect data subjects, such as right of information, access, rectification, complaints, etc. The DPO of the institution or body must play a crucial role in this respect.

Since the regulation conferred powers to the DPOs for investigating matters (point 1 of the annex to the regulation), he/she is an excellent position to treat complaints in a first phase and to try to solve the problem internally.

The EDPS has had the opportunity of giving his advice on the implementing rules drafted by the Court of Auditors, with very satisfactory results.

Several other issues were brought to the attention of the EDPS. This gave the EDPS the opportunity to express his opinion.

One issue concerned the evaluation of military staff by the Council. Although it was concluded that such a processing operation does not fall under the scope of the regulation, the EDPS used the opportunity to advise on the concept of a controller and the applicability of general data protection principles.

Another issue received at the end of 2005 dealt with the publication of photographs of staff members in the intranet of the Commission, using previous photos taken for security badges. In early January 2006 a negative opinion was issued, focusing on the need for the data subject's consent.

A further issue concerned personal data processing by the Court of Auditors in the course of auditing activities. The EDPS considered that this particular data processing falls within the scope of the regulation.

Some general guidelines, including the need for prior checking, were given to the DPO of OLAF on measures to be taken with regard to certain beneficiaries of operations financed by the Guarantee Section of the EAGGF ⁽²¹⁾.

Other informative recommendations were given on various subjects such as the processing of data in the context of group visits to the Court of Justice and the access right concerning assessment of management skills in the European Central Bank.

Finally, as to the role of the DPO's, it should be mentioned that:

- upon request from the DPO of the Commission, the EDPS recommended the appointment of a DPO for each interinstitutional office; this idea was included in the DPO position paper (see paragraph 2.2);
- several bilateral meetings with DPOs have taken place to advise them on several issues of their concern.

3.5. Perspectives for 2006 and further

3.5.1. New technological developments

The European Commission is promoting a European information society, founded on innovation, creativity and inclusion. This society will rely on three major technological trends: an almost unlimited bandwidth, an endless storage capacity and ubiquitous network connections. In this paragraph, the EDPS describes some new technological developments that are likely to take place as a result of these trends and that are expected to have a major impact on data protection.

⁽²¹⁾ European Agriculture Guidance and Guarantee Fund.

Directive 95/46/EC defines personal data as:

‘[...] any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.’

The application of this concept of personal data to emerging technologies might raise new issues, since the meaning of two important elements of the definition of personal data is no longer self-evident. These two elements are ‘relating to’ and ‘identifiable’. The application of these elements is challenged by new forms of processing like web services and by an erosion of the traditional technological barriers (power limitations, limited transmission range, isolated data, etc.). This is well-illustrated by the growing use of RFID tags and the massive development of communication networks which have the following impact:

- all tagged objects become a collector of personal data;
- the ‘presence’ of these smart objects as well as individuals who carry them is characterised by its ‘always on’ nature; and
- the resulting cascade of data continuously feeds an enormous amount of stored data.

RFID, a promising and challenged technology

In 2005, the EDPS contributed to the Article 29 Working Party activities in the field of RFID and welcomed the exploratory steps undertaken by the Commission. However, the critical nature of RFID tags for the protection of personal data demands more in-depth analysis. These technologies are not only critical because of the new way of collecting personal data they are providing, but also because RFID tags will constitute key elements of the ‘ambient intelligent’ environments. To this effect, it is important that consultation meetings are held between all the stakeholders involved.

Ambient intelligence emerging environment

According to the ITU report ⁽²²⁾, released during the UN summit in Tunis, the emerging information society is being built on an ‘Internet of things’, establishing bridges between the digital world and the real world. In such an environment, the data protection model involving a centralised data controller is clearly challenged by the growing ubiquitous network connectivity.

In the transition period, where the user navigates between islands of intelligent environment, it is critical to introduce privacy and data protection requirements as part of the design of these ambient intelligence (AmI) spaces. The domestication of these emerging technologies and therefore their wide acceptance will not only be reached by the attractiveness of AmI worlds for their convenience and the new services they offer, but also by the benefits of well-tailored and consistent data protection safeguards which will have to be implemented. One of the biggest challenges of an AmI world will be to properly manage the data that are continuously produced by these environments.

Identity management systems

Identity management systems are considered to be the key elements of emerging e-government services. These systems will require special attention from the perspective of data protection. Identity management systems can be seen as the conversion into a digital form of two fundamental processes: the identification process and the identity building process. Both processes are based on the use of personal data, like biometric data. The implementation of proper standards plays a determinant role for the compliance of these processes with the data protection legal framework. But the definition of these standards is highly strategic as one of the objectives is to obtain a wide interoperability for the benefits of the mobility principle as part of the Lisbon objectives.

The recent US initiatives which defined a new standard for all the federal employees and contractors will surely have a strong influence on international standards. The EU needs to consolidate the investments already undertaken in this field and launch new initiatives, of course with due respect to the requirements of data protection. Moreover, a consistent data protection framework has contributed to controlling the risks of identity theft, an important threat for identity management systems that has been kept at a relatively low level so far.

⁽²²⁾ ITU Internet reports 2005: *The Internet of things*, November 2005: <http://www.itu.int/osg/spu/publications/internetofthings>.

The biometrics age

The use of biometric data was introduced in numerous proposals of the European Commission in 2005. These first initiatives will facilitate the adoption of biometrics in numerous other aspects of the European citizen's everyday life. The EU institutions therefore have a great responsibility as to the way in which these technologies will be implemented.

In his opinion on the proposals regarding the second generation Schengen information system (SIS II), the EDPS proposed the development of a list of common and elementary requirements based on the inherently sensitive nature of biometric data. This list should be applicable to any system using biometrics, independently of its nature. It should be defined and built by a multidisciplinary panel and go beyond the definition of standards by merely providing implementation methodologies which respect data protection rights of the user. As an illustrative and non-exhaustive list, the EDPS suggested the following elements: a fallback procedure, a targeted impact assessment, emphasis on the enrolment process and awareness on the level of accuracy.

3.5.2. New developments in policy and legislation

Opinions and other interventions

In the last month of 2005, the EDPS received further requests for consultation on Commission proposals in the area of police and judicial cooperation. The EDPS will deliver his opinions in the first months of 2006.

Special attention has to be given to the proposal for a Council framework decision on the exchange of information under the principle of availability, adopted by the Commission on 12 October 2005. This principle, introduced by the Hague programme, entails that information being controlled by national law enforcement authorities in one Member State for the purpose of crime prevention, should be also available to competent authorities of other EU Member States. This proposal is strictly linked to the proposal on data protection in the third pillar.

Moreover, this proposal must be seen in the context of a general trend to increase exchanges of data between law enforcement authorities of EU Member States. Indeed, parallel legal instruments have been proposed in different contexts: the Prüm Convention (sometimes called ‘Schengen III’), signed by seven Member States, is only one example. This confirms the desirability of a comprehensive legal framework for the protection of personal data in the third pillar, independently from the approval of the proposal on the availability principle, as stated in the EDPS opinion on data protection in the third pillar.

Another trend concerns the proposals aimed at extending the investigative powers of law enforcement agencies (frequently including Europol) by granting them access to databases which are not originally developed for law enforcement purposes. The Commission issued on 24 November 2005 a proposal for a Council decision concerning the access for consultation of the visa information system by authorities responsible for internal security and by Europol. The EDPS issued an opinion on this proposal on 24 January 2006. Moreover, the Commission communication on improved effectiveness, enhanced interoperability and synergies among European databases explicitly suggests granting authorities in charge of internal security access to other large-scale databases such as SIS II first pillar data or Eurodac. Needless to say, this is a development that the EDPS intends to monitor very closely, taking into consideration the need for a balance between the core principles of data protection and the interests of the authorities in charge of internal security.

Furthermore, the Commission adopted a proposal for a framework decision on the exchange of information extracted from criminal records. This proposal would lay down organisational measures regulating the storage and the exchange between Member States of information relating to convicted persons. The proposal should replace the ‘urgency measure’ on which the EDPS gave his opinion on 13 January 2005 (see above).

At the end of 2005, the Information Society and Media DG started the process for a review of the EU regulatory framework for electronic communications and services, including the review of Directive 2002/58/EC. The EDPS will closely follow this process and will present his ideas on future regulation in this area.

Mid- and long-term focus

It is clear that the agenda of the EDPS is, for a great part, determined by the work programme of the Commission. The work of the EDPS for 2006 and 2007 must be seen in this perspective: changes in the priorities set out by the Commission can lead to changes in the work programme of the EDPS.

In 2005, the consultative practice of the EDPS has been almost exclusively focused on the area of freedom, security and justice. The background of most of the interventions of the EDPS had to do with growing needs for exchange of information across the internal borders of the Member States for purposes of combating terrorism or other (serious) crime and/or for purposes related to the entry of third-country nationals into the EU territory.

The Commission communication on the annual policy strategy 2006 and the Commission legislative and work programme 2006 establish the priorities for 2006 and, to a lesser extent, the years afterwards. To the EDPS, the perspectives of prosperity and security are the most important. Within these perspectives, the orientations will shift.

- As to prosperity: the EDPS will closely follow the further initiatives towards the development of a European Information Society. In the short term, the review of the regulatory framework for electronic communications calls for attention.
- As to security: within the area of freedom, security and justice, other priorities might become predominant, related to technological developments such as biometrics and the growing pressures on public and private controllers of databases to allow access for law enforcement purposes. In this context, the Commission presented as a key initiative the access by police forces to databases for external border control.

In general, other policy fields will become more important, such as electronic communications and medical data.

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 the directive. Its tasks are laid down in Article 30 of the directive and can be summarised as follows:

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

The 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, and a representative of the Commission. The Commission also provides the secretariat of the working party.

The European Data Protection Supervisor (EDPS) has been a full member of the Article 29 Working Party since early 2004. Article 46(g) of Regulation (EC) No 45/2001 provides that the EDPS participates in the activities of the working party. The EDPS considers this to be a very important platform for cooperation with national supervisory authorities. It is also evident that the working party should play a central role in the uniform application of the directive, and in the interpretation of its general principles. This is another reason why the EDPS is an active participant in the working party's activities.

According to Article 46(f)(i) of the regulation, the EDPS must also cooperate with national supervisory authorities to the extent necessary for the performance of their duties, in particular by exchanging all useful information and requesting or delivering other assistance in the execution of their tasks. This cooperation takes place on a case-by-case basis. The EDPS also contributes to national events on particular issues at the invitation of national colleagues. The direct cooperation with national authorities is growing ever more relevant in the context of international systems such as Eurodac and the proposed visa information system (VIS), which require effective joint supervision (see paragraph 2.8).

The working party issued a number of opinions in 2005 on proposals for legislation which had also been the subject of an opinion of the EDPS on the basis of Article 28(2) of the regulation. This latter opinion is a compulsory feature of the EU legislative process, but the opinions of the working party are of course also extremely useful, particularly since they might contain additional points of attention from a national perspective.

The EDPS therefore welcomes these opinions from the Article 29 Working Party, which have been quite consistent with opinions adopted shortly before by the EDPS. Examples of good synergy between the working party and the EDPS ⁽²³⁾ have been the following:

- Opinion on the proposal for a regulation of the European Parliament and of the Council concerning the visa information system (VIS) and the exchange of data between Member States on short-stay visas (COM(2004) 835 final), adopted on 23 June 2005 (WP 110) ⁽²⁴⁾;
- Opinion on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), adopted on 21 October 2005 (WP 113);
- Opinion on the proposals for a regulation of the European Parliament and of the Council (COM(2005) 236 final) and a Council decision (COM(2005) 230 final) on the establishment, operation and use of the second-generation Schengen information system (SIS II) and a proposal for a regulation of the European Parliament and of the Council regarding access to the second-generation Schengen information system (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final), adopted on 25 November 2005 (WP 116).

⁽²³⁾ See EDPS opinions issued on 23 March, 26 September and 19 October 2005.

⁽²⁴⁾ See the working party's website (http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm).

The EDPS also contributed actively to different opinions of the working party which are designed to promote a better implementation of Directive 95/46/EC or a uniform interpretation of its key provisions. The EDPS strongly believes that such activities should continue to play a prominent role in the working party's annual work programme. Examples of such activities have been:

- the Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification, and the role of data protection officers in the European Union, adopted on 18 January 2005 (WP 106);
- the working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, adopted on 25 November 2005 (WP 114).

It should be noted that common interpretations of the directive may have a direct effect on the application of Regulation (EC) No 45/2001 for Community institutions and bodies, since both instruments are closely related: e.g. Article 26(1) of the directive and Article 9(6) of the regulation are almost identical for transfers to third countries. The EDPS therefore intends to firmly build on these interpretations in his work.

Finally, the EDPS has contributed actively to documents relating to important new technological developments. A typical example was a document on data protection issues related to RFID technology, adopted on 19 January 2005 (WP 105). The EDPS is also represented in the working party's Internet task force.

4.2. Third pillar

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

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

In 2004, an agreement was reached on a structured approach for developing policy positions on policing and related matters. A planning group was established to coordinate the activities of the various bodies, at which the EDPS was represented and, secondly, the Police Working Party was revived as a common platform of the European conference (see also paragraph 4.3). In June 2004, the members of the planning group agreed that the Police Working Party, at which all authorities were to be represented, should prepare:

- a position paper for adoption at the spring conference 2005 in Krakow;
- an opinion on the future legislative instrument on data protection in the third pillar; and
- an opinion on the Swedish proposal for a framework decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

The meeting of the Police Working Party held in The Hague on 28 January 2005 resulted in three documents:

- a draft position paper on law enforcement and information exchange in the EU, containing concrete proposals for drafting a third pillar instrument on data protection, ensuring consistency with the data protection standard of Directive 95/46/EC;
- a draft ‘Krakow declaration’ calling for a data protection system for the third pillar, in line with the standard of the directive and presenting the position paper as a contribution to the current initiatives;
- a draft opinion on the Swedish proposal.

At a public hearing at the European Parliament’s LIBE Committee on 31 January 2005, several speakers, including the EDPS, advocated adequate specific rules for the third pillar. The data protection authorities met again on 12 April 2005 to finalise the documents to be submitted to the spring conference in Krakow.

The spring conference held from 24 to 26 April 2005 adopted the three abovementioned documents. In its ‘Krakow Declaration’ ⁽²⁵⁾, the conference stated that ‘initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection’.

On 21 June 2005, a meeting of the Police Working Party was held in Brussels to discuss the reactions received on the ‘Krakow declaration’, the position paper and the opinion on the Swedish initiative. In addition, it was also informed by representatives of the Commission on the state of play of the framework decision on data protection in the third pillar. The Commission presented a discussion paper on this subject. The topic of right of access to police data was also addressed, following discussions which had taken place during the spring conference ⁽²⁶⁾.

On 4 October 2005, the Commission adopted a proposal for a framework decision on data protection in the third pillar, on which the EDPS issued an opinion on 19 December 2005 (see also paragraph 3.3.1).

The Police Working Party met again in Brussels on 18 November 2005 to start preparing an opinion on the final Commission proposal. The participants broadly agreed that this proposal represents a milestone in data protection and that the possibility to have data protection in the third pillar should not be forgone. Much of the discussion focused on the scope and legal basis of the proposal. The EDPS has taken a firm position on both subjects in his opinion on the proposal.

The discussions also addressed the draft framework decision on the availability principle as well as the results of a questionnaire on the right of access. The questionnaire highlighted the differences among Member States in granting right of access to police data. The conclusions of the questionnaire support the need for harmonisation, especially with a view to the increasing exchange of data between Member States.

⁽²⁵⁾ See the website (http://www.edps.eu.int/02_en_legislation.htm#EDPC).

⁽²⁶⁾ Further to the Commission’s discussion paper on data protection in the third pillar, the working party commented on this document and forwarded its comments to the relevant service of the Commission in July 2005

At a special meeting in Brussels on 24 January 2006, the Conference of European Data Protection Authorities adopted an opinion on the proposal for a framework decision on data protection in the third pillar. This opinion is quite consistent with the opinion of the EDPS which was adopted on 19 December 2005 (see paragraph 3.3.1). The need for further steps is likely to be discussed at the next spring conference.

SIS II

The EDPS also cooperated with the Schengen JSA when drafting the opinion on the second generation of the Schengen information system (SIS II). Informal contacts took place regularly in order to coordinate to the greatest possible extent the relevant approaches in this case. The EDPS highly appreciated being invited as an observer to a meeting of the Schengen JSA on 27 September 2005, and took the opportunity to clarify his position on certain points. Early in 2006, follow-up discussions with the Schengen JSA resulted in a common approach to the supervision of SIS II, which deserves to be taken into account by the European Parliament and the Council in their decisions about the SIS II proposals.

4.3. European conference

Data protection authorities from Member States of the EU and the Council of Europe meet annually for a spring conference to discuss matters of common interest and to exchange information and experiences on different topics. The EDPS and the Assistant EDPS took part in the conference in Krakow from 24 to 26 April 2005 hosted by the Polish Inspector General for Data Protection.

The EDPS specifically contributed to the session entitled ‘Directive 95/46/EC: amendment or new interpretation’. Other subjects dealt with at the conference were: ‘The impact of Directive 95/46/EC on personal data protection in the EU and third countries’, ‘The impact of the jurisprudence of the European Court of Justice on the application of Directive 95/46/EC’, ‘Transfer of personal data to third countries — binding corporate rules — the new legal instruments — applicable law’, ‘Personal data protection officials’, ‘The right of access to data executed by data subjects — practical approach’, ‘Awareness and education’ and ‘The protection of personal data in the third pillar’. In this context (see paragraph 4.2) a number of important documents were adopted.

The next European conference will be held in Budapest on 24 and 25 April 2006, and will deal inter alia with ‘Data protection in the third pillar’, ‘Data protection for historical and scientific research’ and ‘Effectiveness of data protection authorities’. The EDPS will chair the session on ‘Data protection in the third pillar’.

4.4. 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 September for many years. The 27th International Conference on Privacy and Data Protection was held in Montreux, Switzerland, from 14 to 16 September 2005.

The general theme of the 27th conference was ‘The protection of personal data and privacy in a globalised world: a universal right respecting diversities’. The EDPS and Assistant EDPS both attended the conference. At the end of the conference, the participating authorities agreed to promote the recognition of the universal character of data protection principles and adopted the ‘Montreux declaration’⁽²⁷⁾. The declaration sums up these principles and calls on various stakeholders to contribute to their universal recognition both in political, legal and practical terms. The realisation of the objectives of this declaration will be assessed on a regular basis.

The conference also adopted two resolutions on the use of biometrics in passports, identity cards and travel documents, and on the use of personal data for political communication. Both deal with subjects which currently give rise to complicated discussions in many jurisdictions⁽²⁸⁾.

The next international conference was to take place in Buenos Aires from 1 to 3 November 2006, but will probably be held at an alternative location soon to be decided.

⁽²⁷⁾ See the website: http://www.edps.eu.int/02_en_legislation.htm#international.

⁽²⁸⁾ Ibid.

4.5. Workshop for international organisations

The EDPS hosted a workshop on data protection in international organisations, held in Geneva on 15 September 2005, in partnership with the Council of Europe, the OECD and the Swiss and Austrian data protection authorities. It gathered representatives of some 20 international organisations, such as the UN, Interpol, the IOM and NATO. The objective was to raise awareness of universal data protection principles and their practical consequences for the work within international organisations. Its title was ‘Data protection as part of “good governance” in international organisations’.

Although virtually all international organisations process personal data and many even sensitive data, mostly in the interest of and to the benefit of the data subjects, there are very often insufficient safeguards. The reason for this lack of safeguards is that international organisations are in many ways exempted from national laws, and thus not legally bound by the wide range of data protection instruments that are applicable to public bodies and private companies in many countries around the world. The workshop aimed at highlighting this shortcoming with a view to resolving the situation. It was highly appreciated by the participants, many of which asked for a follow-up. This will be looked into in due course with international organisations able and willing to cooperate and share experience in this field.

5. COMMUNICATION

5.1. Introduction

The year 2005 brought a significant qualitative step in the external communications of the EDPS with the development of an information strategy. Expanding on the methods elaborated during the first year of the Office, the strategy aims to structure the communications in relation to a global as well as a specific objective. It does so by defining the communication tools at hand and by relating the target groups to the main activities of the institution.

The global objective is twofold:

- to raise data protection awareness generally;
- to raise awareness of the EDPS and the institution's main activities.

General awareness raising is important during the first years of activity of an institution and the EDPS devoted particular attention to putting the institution on the political map. The EDPS and the assistant EDPS, therefore represented the institution at numerous conferences, seminars and lectures — not only at the main headquarters of the EU institutions and bodies, but also in a number of Member States, such as Cyprus, France, Germany, Lithuania, Poland, Spain and the UK. Also non-Member States, such as the USA and Switzerland were visited in this context — for a high-level round table discussion on data privacy and for the annual International Conference on Privacy and Personal Data Protection, respectively.

As work with different dossiers (such as prior checks and consultation on legislation) progressed, the global objective was increasingly transmitted in the context of a specific objective. The specific objective is linked somewhat more to a particular case. Such examples may be found in the presentation at the Council of the opinion on the proposal for a framework decision on data protection in the third pillar and in the presentation in the European Parliament of the opinion on the proposal for a directive on retention of electronic communication data.

5.2. Main activities and target groups

With the elaboration of the information strategy, different target groups were identified. In relation to the three main activities of the EDPS, they are indicated below.

1. Supervision — making sure that the EU administration respects its data protection requirements
 - (a) The individual: data subjects in general, depending on the processing operation involved, and staff of the EU institutions and bodies in particular. This target group focuses on the 'rights perspective'; the fundamental right to data protection and the specific rights of the data subjects (notably laid down in Articles 13-19 in the regulation);

(b) The institutional system: the DPOs, data protection controllers (DPCs) and the controllers in the EU institutions and bodies. This focuses on the ‘obligations perspective’, such as the general rules on lawful processing, the criteria for making processing legitimate, and also on the obligation to provide the data subject with information on the processing (as laid down in Articles 4 to 12 of the regulation).

2. Consultation — promoting data protection in new legislation and administrative measures

Thus far, the EDPS has given advice in relation to proposals for new legislation and the target groups have been what can be referred to as ‘EU political stakeholders’. Following the legislative procedures in the EU, EDPS advice on a given proposal has thus initially been directed to the European Commission (because of the numerous proposals in the law enforcement field in 2005, most of the advice concerned the Justice, Freedom and Security DG, although also other DGs have been affected). In the second stage, when the Council and the European Parliament scrutinise the proposal, the EDPS advice has been directed to, for instance, the Council’s Article 36 Committee and the LIBE Committee of the Parliament.

3. Cooperation

The EDPS cooperates with other relevant actors in the field, grouped together as ‘data protection colleagues’. Three levels of cooperation can be discerned: with colleagues on the EU level, with colleagues in a broader European context (such as in the framework of the European Data Protection Conference, which also includes non-EU members of the Council of Europe), or at the international level (such as in the framework of the International Data Protection Conference).

At the EU level, the cooperation can be divided into work within the first pillar (the area of the EC Treaty) and work within the third pillar (police and judicial cooperation). The most important forum for the first pillar is the Article 29 Working Party (see paragraph 4.1).

As concerns the third pillar, the EDPS has participated as an observer in a number of joint supervisory bodies (see also paragraph 4.2). When the proposals for SIS II were discussed in the joint supervisory authority for Schengen, the EDPS participated in those discussions and also sent his opinion to the president and the secretariat.

5.3. Communication tools

The year 2005 also saw the development of a set of communication tools, such as background papers, the newsletter, press releases, etc. which is customary for many public bodies. Each of these tools has its own characteristics and lifecycle, and their use may vary according to the target group to which it is addressed. The most important elements are described below.

5.4. The EDPS information campaign

Spanning from March to July, the EDPS distributed the two descriptive brochures that were developed at the end of 2004 (one focusing on the institution and its tasks and one focusing on the rights of the data subjects). The brochures were translated into all 20 official languages of the EU and, all in all, some 80 000 copies were circulated throughout the Member States. The target groups were addressed directly (each EU staff member received his/her own copies) or indirectly, distributing copies through the Europe Direct information relays and the data protection authorities in the Member States.

5.5. The press service

Immediately prior to the launching of the background paper on public access to documents and data protection, the EDPS press service was established. The service is run by a press officer, who is the contact person for journalists and who is responsible for dealing with requests for interviews, organising press conferences, editing press releases, etc.

Naturally targeting journalists, the press service aims at promoting a specific message, directed towards one, or several, target groups. Media is in that sense a target group as well as a relay that can help to forward the message to the target group(s) in question.

Press conferences were organised for the presentation of the annual report in March and for the presentation of the EDPS opinion on data retention in September 2005. Both were well attended and resulted in significant media coverage. A press lunch was organised for the presentation of the background paper on public access to documents and data protection (see paragraph 2.6) and for general background on EDPS activities and priorities.

5.6. The website

Considered as the most important tool of communication for the EDPS, the website is the most complete source of information on the activities of the institution. It also offers the possibility to interlink information and provide further explanations through cross references.

The website was established during the first half of 2004 and grew considerably during 2005 with new sections and new types of documents. Without advanced statistical tools, it is difficult to draw dependable conclusions on the use of the website. Nevertheless, some general impressions are that:

- there was a quantitative leap in the number of visits after the summer holidays in August, when traffic stabilised around 1 000 visits per week, compared to the preceding average of around 700 per week;
- an average of two pages per visit (3.3 if the count excludes visitors who only view one page, for instance by the use of a direct link to a particular online document), was indicated — thus pointing to a low ‘surfing tendency’;
- each time the EDPS presented a new opinion, a newsletter, a press release or something similar, there was a definite increase in the use of the website.

The statistics further motivated the EDPS to engage staff in a project that will result in a second, more user friendly, generation of the website. The remake project, which started during the autumn of 2005, will finish by spring 2006 with the launch of the new website.

5.7. Speeches

The EDPS continued to invest considerable time and effort in explaining his mission and raising awareness about data protection in general, and a number of specific issues, in speeches for different institutions and in various Member States throughout the year. The EDPS also gave a number of interviews to relevant media.

The EDPS frequently appeared in the European Parliament's LIBE Committee. On 31 January he presented his views on 'third pillar' issues at a public seminar about 'Data protection and citizens' security'. On 30 March he presented his opinion on the proposal for a regulation concerning the visa information system (VIS) at the public seminar 'Borders'. On 12 July he explained the background paper on 'Public access to documents and data protection'. On 26 September he presented his opinion on the proposal for a directive on retention of communications data, and on 23 November he presented his opinion on the proposals concerning the second-generation Schengen information system (SIS II).

On 21 October the opinion on SIS II was presented by the Assistant EDPS to the Schengen *acquis* working group of the Council.

On 18 October the EDPS delivered a speech at a Commission symposium on e-security, about the implementation of Regulation (EC) No 45/2001. On 9 November he gave a lecture in Council about the need for data protection under the title 'Is Big Brother watching?' On 15 December he gave a similar lecture at the Commission.

In March, the EDPS delivered a series of speeches in Canada and the USA: on 5 March at the University of Ottawa, on 7 March at the University of Michigan Law School in Ann Arbor (USA); and on 10 March at a conference of the International Association of Privacy Professionals (IAPP) in Washington DC. On 8 June, the EDPS participated in a meeting of privacy and information commissioners in Ottawa at the invitation of the Privacy Commissioner of Canada.

In the course of the year, the EDPS also visited a number of Member States. On 7 April he was at the European Academy for Freedom and Information and Data Protection, in Berlin. On 11 April he was at the farewell of the Data Protection Commissioner of Sachsen-Anhalt in Magdeburg, Germany. On 18 April, he lectured at the University of Leiden, the Netherlands. On 25 April he spoke at the European conference in Krakow, Poland. On 2 June he attended the Nordic conference in Trondheim for discussions with Scandinavian colleagues. On 23 June he presented a speech on 'Data protection and security in the EU' at the 14th Data Protection Forum in Wiesbaden.

On 13 October, the EDPS was at the University of Tilburg, the Netherlands. On 21 October he gave a presentation at Biometrics 2005 in London. On 2 November, he delivered a speech in Limassol, Cyprus. On 8 November he participated in a seminar in the French Senate in Paris. On 14 November he spoke at a conference on e-commerce, in Vilnius, Lithuania. On 29 November he contributed to a conference in Manchester and on 30 November he was at a seminar on ‘Directive 95/46/EC: 10 years later’ at the British Institute of International and Comparative Law, in London.

The Assistant EDPS made similar presentations in Madrid and Barcelona, inter alia for the European judicial network, on data protection in the third pillar.

5.8. Newsletter

A first issue of the EDPS newsletter was sent to a number of people who were considered as relevant receivers, for instance journalists and people who work within the data protection field. The newsletter aims at highlighting recent activities and promoting documents that are available online on the website. Three issues were released during the second half of 2005, and at least four issues are envisaged per year.

The possibility to subscribe ⁽²⁹⁾ to the newsletter was introduced at the end of October, and some 250 people did so during the two months that followed; these included Members of the European Parliament, EU staff and staff of the national data protection authorities.

5.9. Information

During 2005 the EDPS received more than 100 e-mail requests, mostly from private citizens but also from lawyers, students, etc., for information and/or advice on data protection in Europe. Considering these requests as a good opportunity to provide a service, the EDPS has set the objective to provide an individually tailored reply within a couple of working days — which is achieved most of the time. The requests can be divided into two main categories — requests for advice and requests for information, although some of them naturally contain elements of both.

⁽²⁹⁾ http://www.edps.eu.int/publications/newsletter_en.htm

More than 30 requests for advice were dealt with, ranging from specific questions on the interpretation of a certain article or a special element in EU legislation on data protection, through what should be included in a privacy statement on a website of an EU institution, to questions on the differences between general principles of data protection in the EU versus the USA.

The EDPS thus also dealt with some 70 requests for information — a wide category that comprises, inter alia, general questions on EU policies, questions on new legislation and questions on data protection that are publicly debated, as well as questions relating to the situation in a particular Member State. This, for the moment relatively low number of requests, has allowed the office to provide somewhat more individualised answers that highlight relevant aspects and also inform of, for instance, related documents adopted by the Article 29 Working Party.

Most of the requests received were either in English or in French; but there were also a sizeable number of requests in other ‘old’ and ‘new’ languages. In those cases where it was necessary, the replies of the EDPS were translated, so as to provide adequate information in the mother tongue of the person contacting the EDPS. The requests have also been used as the basis for the editing of a ‘frequently asked questions’ section, which will be added to the website during 2006.

5.10. Logo and house style

A project aimed at creating a new logo and an accompanying new house style started in October. The work initially focused on the development of a logo that would have a clear ‘EU institutional’ link but still would stand out as individual, while having a clear visual link with the main responsibilities of the EDPS. The new logo has been gradually introduced since its finalisation in mid-December 2005.

The new logo is based on the yellow and blue colours of the EU flag and it takes the shape of a dynamic storage disk, which can also be seen as a protective shield for the data. Pixels of information form an ellipse that transforms from the shape of a person to European stars.

The development of the house style will continue throughout the first months of 2006 and will result in a completely revised visual identity that will be used throughout the wide range of communication tools, such as letters, opinions, papers, the newsletter and website.

5.11. Visits

As part of the work of increasing the visibility of the EDPS, visits were received from two groups of students specialising in EU affairs. These visits were highly appreciated, and more prominence to this possibility will be given in the remake of the website.

6. ADMINISTRATION, BUDGET AND STAFF

6.1. Introduction: continuing to establish the new institution

The setting up of the EDPS as a new institution continued on the basis established in 2004, with the aim of consolidating its positive start. In 2005, the EDPS gained additional resources both in terms of his budget (which grew from EUR 1 942 279 to EUR 2 879 305) and his staff. As regards staffing, two new programmes were launched enabling trainees and national experts to be recruited.

Collaboration with the institutions (the European Parliament, the Council, and the European Commission) which signed the administrative cooperation agreement of 24 June 2004 was further improved and extended also to other services, allowing for considerable economies of scale. Slower performance of some tasks, connected to the principle of shared assistance (Commission–Parliament) was noted, but that should be resolved in 2006 with the cooperation of staff from the institutions concerned. The EDPS took over some of the tasks which were originally performed by other institutions (for example the purchase of furniture).

The administrative environment is gradually being developed on the basis of priorities, taking account of the needs and size of the institution. The EDPS has adopted various internal rules necessary for the proper functioning of the institution, in particular a system of standards for internal control and implementing provisions for the Staff Regulations.

The premises originally made available to the EDPS are now not large enough, and the European Parliament has been approached to obtain larger premises.

6.2. Budget

A budget estimate for the year 2005 was drawn up in March 2004 with the support of European Parliament staff, at a time when the EDPS was just beginning to get established. The budget adopted by the budgetary authority for 2005 was EUR 2 879 305. This represents a 48.8 % increase compared with the 2004 budget (over 11 months). It was calculated on the basis of parameters set by the Commission and on the basis of the budgetary authority's policy guidelines. An amended budget was adopted following the budgetary authority's decision to adjust salaries and pensions for 2005. According to EU amended budget No 2, adopted for the 2005 financial year on 13 July 2005, the budget for 2005 was EUR 2 840 733.

A new budget line was created without financial implications. Not previously planned, it enables to cover services provided by people not connected with the institutions, including 'interim' staff, where necessary.

Since the EDPS staff is so limited, it hardly seemed efficient to draw up internal rules specific to it. This is the reason why the EDPS decided to apply the Commission's internal rules for the implementation of the budget, insofar as those rules are applicable to the structure and scale of the EDPS and where specific rules have not been laid down.

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

In its report on the 2004 financial year, the Court of Auditors stated that the audit had not given rise to any observations.

6.3. Human resources

The EDPS benefits from very effective assistance from Commission staff, regarding tasks relating to the personnel management of the institution (which includes the two appointed members and staff).

6.3.1. Recruitment

As a new institution, the EDPS is still in a building phase, and will be so for some years to come. The EDPS is taking its place in the Community environment, and its growing visibility is having the effect of increasing the number of tasks it has to perform. The significant growth in 2005 of the workload has been described above. Naturally, human resources have a fundamental role to play in supporting this process.

Nevertheless, the EDPS has chosen initially to restrict expanding in tasks and staff, using controlled growth to ensure that new subjects are fully taken on board and that new staff are adequately integrated and trained. For that reason, the EDPS called for the creation of just four posts in 2005 (two A, one B and one C). This request was authorised by the budgetary authority, with the number of staff increasing from 15 in 2004 to 19 in 2005. Vacancy notices were published in February 2005, and four new colleagues were employed. The recruitment was carried out on the basis of the rules in force in the institutions: priority was given to transfers between institutions, followed by consultation of the reserve lists and, finally, spontaneous applications from people external to the European institutions and bodies were considered. Of the new colleagues, two are officials and two are temporary staff.

The Commission's assistance in this area has been valuable, particularly the assistance of the Pay Masters Office (PMO) — in establishing entitlements, paying salaries, calculating and paying allowances and various contributions, missions, etc. — and of the Medical Service. The following aspects of the recruitment procedure are now wholly handled by the EDPS: the management of applications and access to EPSO lists, the organisation of interviews, the preparation of recruitment files for those selected, and the creation of the file with all the supporting documents and its transmission to the PMO for entitlements to be established. The excellent working relationship with institutions other than the abovementioned, in particular with the Committee of the Regions and the Ombudsman, should be highlighted here; and this has made possible the exchange of information and best practice in this area.

The EDPS has access to the services provided by EPSO and participates in the work of its management board, as an observer at present. Negotiations on full participation are under way.

6.3.2. Traineeships programme

A significant achievement of 2005 was the creation of a traineeship programme, set up by a decision of 27 May 2005 which was published on the website. The decision is similar to those of the other European institutions, particularly that of the Commission, adapted to suit the size and needs of the EDPS.

The main objective of the programme is to offer recent university graduates the opportunity to put into practice the knowledge acquired during their studies, particularly in their specific areas of competence, thus acquiring practical experience of the day-to-day activities of the EDPS. As a result, the EDPS will increase its visibility to younger EU citizens, particularly university students and young graduates specialising in data protection. In addition to the main traineeship programme, special provisions have been established to accept university students and PhD students for short-term, non-remunerated traineeships. This second part of the programme gives young students an opportunity to conduct research for their thesis, under specific limited admission criteria, in accordance with the Bologna process and the obligation for university students to complete a traineeship as part of their studies.

The main programme hosts between two and three trainees per session, with two five-month sessions per year. The first session of the programme started in October 2005, ending in February 2006.

Extensive experience and resources are needed for the practical organisation of a traineeship programme. The EDPS receives administrative assistance from the Traineeship Office of the Education and Culture DG, which manages all traineeship programmes for the Commission. A service-level agreement has been arranged between the two parties in order to define the details of the assistance. Additionally, the EDPS cooperates with the traineeship offices of other European institutions, including the Council, the Committee of the Regions and the European Economic and Social Committee, particularly in organising visits.

The results of the first three months of the traineeship for the first three EDPS trainees have been extremely positive. The level of selected trainees was high; during the selection process the skills and background of candidates were carefully evaluated, with particular attention being paid to specialisation in the field of data protection. The trainees contributed both to theoretical and practical work, at the same time gaining first-hand experience and on-the-job training on data protection issues as well as first-hand knowledge of the EU institutions.

6.3.3. Programme for seconded national experts

In a decision of 10 November 2005, the EDPS adopted provisions on the rules applicable to national experts seconded to his staff.

The secondment of national experts enables the EDPS to benefit from their professional skills and experience, particularly in the field of data protection, where the necessary expertise is not always immediately available in the various languages. This programme also enables national experts to familiarise themselves with European knowledge and practices in this area. At the same time, the EDPS increases its visibility in the field at operational level.

The EDPS decision on seconded national experts is based on the corresponding Commission decision. However, some changes have been made to the recruitment process to reflect the size of the EDPS and the specific skills required to work in the field of data protection. The EDPS has a policy of recruiting seconded national experts in the framework of official contacts with the Member States, directly addressing the national data protection authorities (DPAs). National permanent representations are informed of the programme and are invited to assist in seeking suitable candidates.

A special mention should be made of the Personnel and Administration DG of the Commission, which provides administrative assistance for the organisation of the programme.

6.3.4. Organisation chart

The EDPS's organisation chart has essentially remained the same since 2004: one unit, with five members, is responsible for administration, staff and the budget; the rest of the team, which is responsible for operational tasks connected with data protection, consists of 14 people and works directly under the direction of the Supervisor and the Assistant Supervisor. Some flexibility has been maintained in allocating tasks to staff, since those tasks are still evolving.

6.3.5. Training

The EDPS staff has access to general and language training courses organised by the Commission and to the courses run by the European Administrative School (EAS). An agreement has been signed with the EAS, laying down the conditions for participation by EDPS staff in the training provided by the school, and the EDPS is currently an observer on its management board. The EDPS has begun consultations with the founding members of the school with a view to participate as a member on the same conditions as the founding institutions.

6.4. Consolidation of cooperation

6.4.1. Follow-up to the administrative cooperation agreement

In 2005, interinstitutional cooperation continued in areas where the EDPS is assisted by the other institutions, by virtue of the **administrative cooperation agreement** with the Secretaries-General of the Commission, the Parliament and the Council, concluded on 24 June 2004. This cooperation is of considerable added value to the EDPS, since it gives it access to expertise in the other institutions in the areas where assistance is provided and allows for economies of scale.

There has been cooperation with various Commission DG's (mainly the Personnel and Administration DG, the Budget DG and the Office for the Administration of Individual Entitlements, but also the Education and Culture DG and the Employment, Social Affairs and Equal Opportunities DG), with the European Parliament (IT services, particularly with arrangements for the second generation of the website, fitting out of the premises, building security, printing, mail, telephone, supplies, etc.) and with the Council (translations).

To facilitate cooperation between Commission departments and the EDPS, direct access from EDPS premises to the Commission's main human resources and financial management software (SIC, Syslog, SI2, ABAC, etc.) has been requested. Such direct access would improve the exchange of information and make it possible for files to be managed more effectively and rapidly by both the EDPS and the Commission. Access has been possible for SI2 and partially for Syslog, but not as yet for the other software. Problems connected with the differing IT environments of the institutions which assist the EDPS in these areas have slowed down this process. It is hoped that it will be completed during 2006.

Service-level agreements (see Annex H) have been signed with the various institutions and their departments. These include the following.

- The agreement with the Council, which provides the EDPS with outstanding assistance — as regards both the speed and the quality of the work — in translation. As the EDPS has increased in visibility, the number of documents to translate has increased. However, the EDPS attempts to limit the number of translations requested as far as possible.
- The agreement with the Commission's Traineeships Office (Education and Culture DG) which enabled the first traineeship programme at the EDPS to be launched in 2005.
- The agreement with the Employment, Social Affairs and Equal Opportunities DG of the Commission to provide the EDPS with the necessary technical assistance to create a portable stand and other additional services for the EDPS (elaboration of a logo, new presentation of the website, etc.).

6.4.2. Interinstitutional cooperation

The EDPS has launched discussions with the European Network and Information Security Agency (ENISA) in view of an administrative assistance agreement. This agreement is to define the implementing arrangements for the security audit of the Eurodac database and the conditions for the conduct of this cooperation (see paragraph 2.8).

Participation in the interinstitutional call for tenders for furniture was a first step by the EDPS towards some autonomy as regards fitting out its office space. The aim of the call for tenders was to conclude various framework contracts for the supply of furnishings.

As a new institution, the EDPS has been invited to participate in various interinstitutional committees and bodies; however, because of its size, such participation had to be limited in 2005 to just a few of them. This participation increased the visibility of the EDPS in other institutions, and encouraged the continuing exchange of information and good practice.

6.4.3. External relations

The process of having the institution recognised by the Belgian authorities has been completed, enabling the EDPS and its staff to have access to the privileges and immunities laid down in the ‘Protocol on the privileges and immunities of the European Communities’.

6.5. Infrastructure

The general infrastructure has been improved upon during 2005. However, with the increased number of staff and further increase expected in 2006, the EDPS is experiencing office space problems, which are hoped to be resolved by acquiring additional space in 2006.

The secure protection of the sixth floor of Rue Montoyer 63 has been of the utmost importance, considering the sensitivity of the data that the EDPS processes.

On the basis of the administrative cooperation agreement, by which European Parliament staff assist the EDPS with its premises, initial furnishings were provided by the Parliament in 2004. This assistance ended in 2005.

6.6. Administrative environment

6.6.1. Establishment of internal control standards

On the basis of the interinstitutional agreement of 24 June 2004, the Internal Auditor at the Commission was appointed as the Auditor at the EDPS.

By his decision of 7 November 2005, and in accordance with Article 60(4) of the financial regulation of 25 June 2002, the EDPS decided to establish internal control procedures specific to the EDPS.

Because of the structure and size of the institution and because of its activities, the EDPS has adopted standards appropriate to the needs of the institution and the risks associated with running the activities, with the possibility of an annual review to take account of how the activities evolve. These standards relate especially to the overall organisation of the institution which, given its size and the nature of the budget to be managed and also given the simplicity of the financial flows established for financial management, mainly covers the administrative functioning of the institution, .

6.6.2. Setting up of the interim staff committee at the EDPS

An **interim staff committee** was set up in 2005. It was consulted on an initial series of general implementing provisions for the Staff Regulations and on other internal rules adopted by the institution (such as its flexitime system).

On 8 February 2006, in accordance with Article 9 of the Staff Regulations of Officials of the European Communities, the Supervisor adopted a decision to establish a staff committee at the EDPS. The elections to form a **definitive staff committee** will take place in March 2006. In the meantime, operational and organisational rules for the committee have been adopted by a general staff assembly.

6.6.3. Flexitime

As a new institution and in the spirit of the reform of the Staff Regulations, the EDPS wanted to give his staff modern working conditions such as flexitime. Flexitime is not an obligation under the Staff Regulations; it is rather a measure to organise the working day with the aim of allowing the staff to reconcile their professional and private lives and also of enabling the EDPS to arrange working hours depending on his priorities. Every staff member is able to choose between traditional hours and flexitime, with the possibility of recovering overtime worked.

6.6.4. Internal rules

A first group of internal rules, necessary for the proper functioning of the institution, and general implementing provisions for the Staff Regulation were adopted (see Annex H). Where these provisions concern subjects on which the EDPS benefits from the assistance of the Commission, they are similar to those of the Commission, with some adjustments to allow for the special nature of the EDPS Office. In some cases, additions have had to be made to some agreements (for example, an additional clause was needed in the Commission's accident insurance contract for the EDPS, to cover seconded national experts). All these provisions are forwarded for information to new colleagues when they arrive.

6.7. Objectives for 2006

As the objectives set for 2005 have been achieved, the EDPS can now move on to a new stage, to consolidate what has been achieved and develop some activities further. This has been made possible by the budgetary authority's agreement to recruit five new colleagues in 2006, and the adoption of a budget of EUR 3 447 233.

Continuing administrative cooperation will nevertheless remain an essential factor in the EDPS's development. The size of the institution does not yet allow it to take on the various tasks currently carried out by the Commission, the Parliament and the Council on its behalf. For this reason, the EDPS intends to request for an extension of the administrative cooperation agreement which expires at the end of 2006.

In 2006 an internal data protection post will be created and a DPO appointed.

The performance indicators adopted in 2005 will be fully implemented, and the EDPS will continue to develop his administrative environment; particular attention will be paid to the development of social activities.

The negotiations which are currently under way to obtain additional office space should lead to a further establishment phase in the first half of 2006.

1. ANNEXES

- A. Extract from Regulation (EC) No 45/2001
- B. List of abbreviations
- C. List of data protection officers
- D. Prior-checking handling time per case and per institution
- E. List of prior-check opinions
- F. List of opinions on legislative proposals
- G. Composition of the EDPS Secretariat
- H. List of administrative agreements and decisions

1.1. Annex A — Extract from Regulation (EC) No 45/2001

Article 41 — European Data Protection Supervisor

1. An independent supervisory authority is hereby established referred to as the European Data Protection Supervisor.

2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies.

The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47.

Article 46 — Duties

The European Data Protection Supervisor shall:

- (a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;
- (b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;
- (c) monitor and ensure the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;
- (d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;
- (e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

- (f) (i) cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that Directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body;
- (ii) also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;
- (g) participate in the activities of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of Directive 95/46/EC;
- (h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b), (4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);
- (i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the Data Protection Officers under Article 26;
- (j) carry out a prior check of processing notified to him or her;
- (k) establish his or her Rules of Procedure.

Article 47 — Powers

1. The European Data Protection Supervisor may:
 - (a) give advice to data subjects in the exercise of their rights;
 - (b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where 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.

1.2. Annex B — List of abbreviations

API	advance passenger information
CDR/REC	career development review system / rapport d'évolution de carrière
CS-VIS	central visa information system
DPC	data protection coordinator
DPO	data protection officer
EAGGF	European Agricultural Guidance and Guarantee Fund
EAS	European Administrative School
EC	European Communities
ECHR	European Convention on Human Rights
EPSO	European Personnel Selection Office
EU	European Union
EUMC	European Monitoring Centre on Racism and Xenophobia
LIBE	Committee on Civil Liberties, Justice and Home Affairs (of the European Parliament)
ITU	International Telecommunication Union
NI-VIS	National Interface Visa Information Office
OHIM	Office for Harmonization in the Internal Market (Trade Marks and Design)
OLAF	European Anti-fraud Office
PNR	passenger name record
RFID	radio frequency identification
SIS	Schengen information system
TCEU	Translation Centre for the Bodies of the European Union
VIS	visa information system

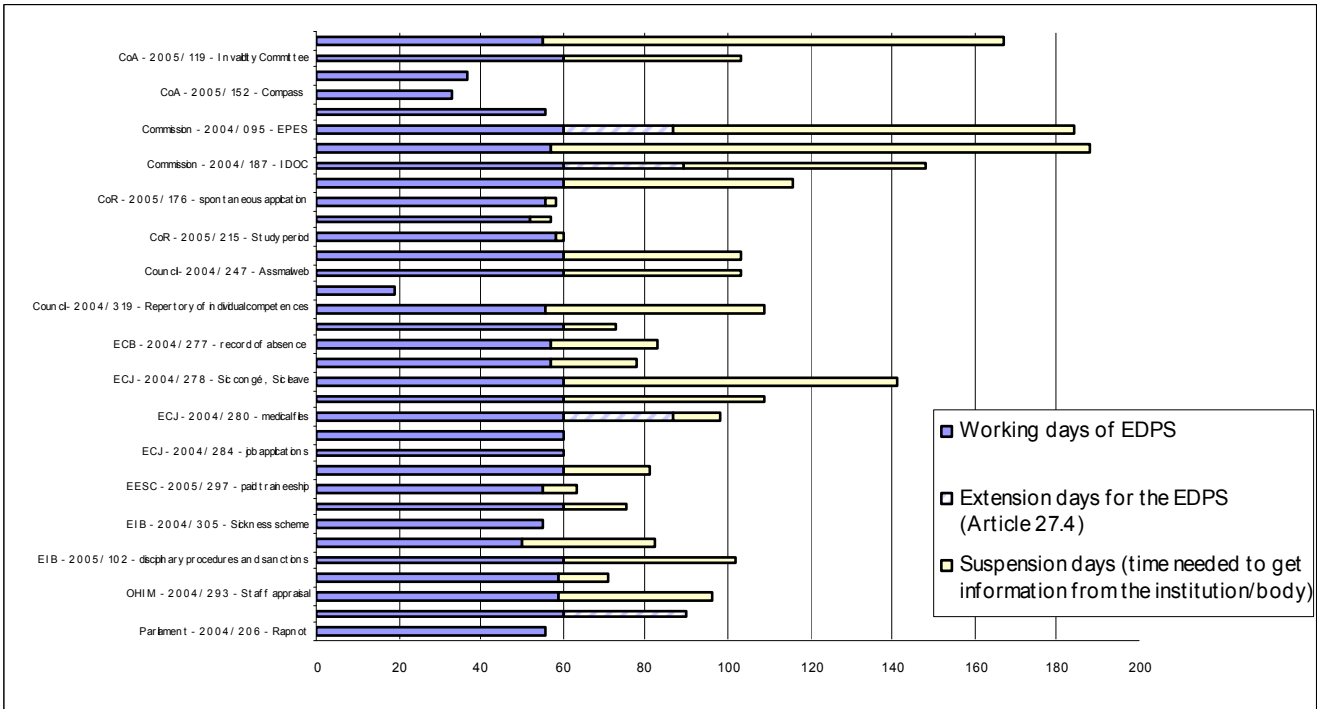
Annex C — List of data protection officers

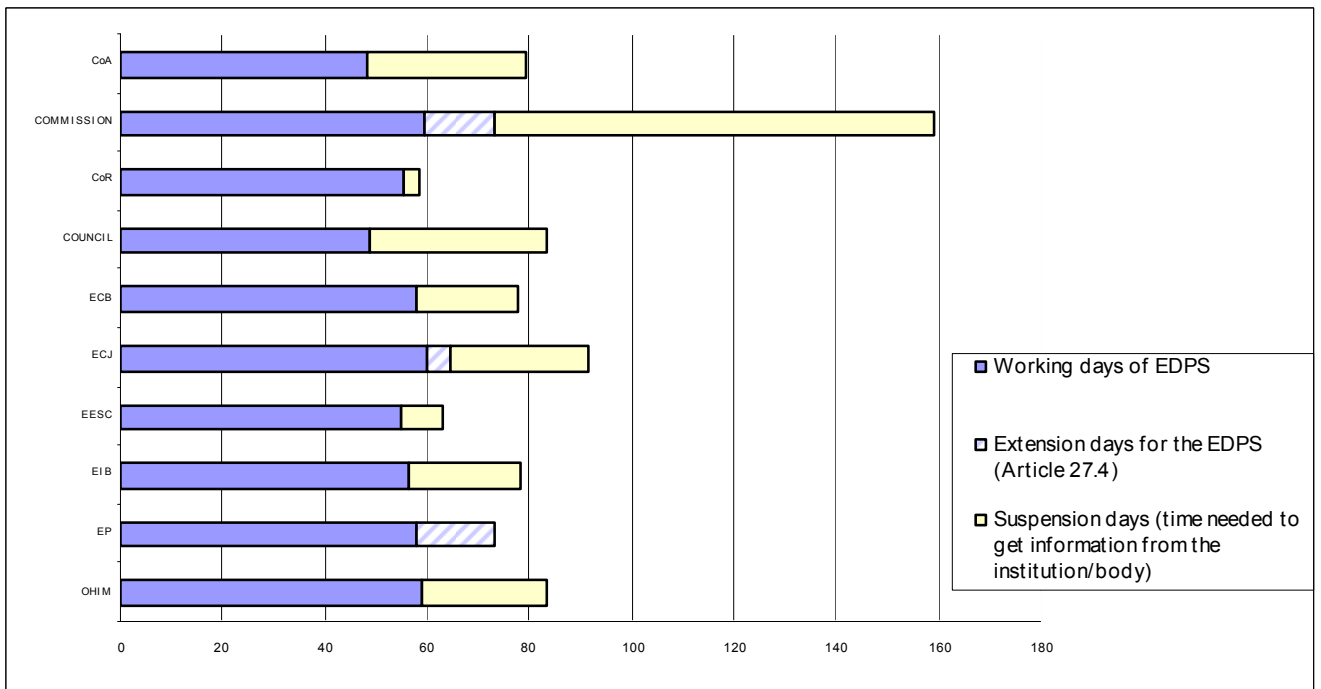
Organisation	Name	E-mail
European Parliament	Jonathan STEELE	DG5DATA-PROTECTION@europarl.eu.int
Council of the European Union	Pierre VERNHES	data.protection@consilium.eu.int
European Commission	Nico HILBERT (Acting Data Protection Officer)	Data-Protection-Officer@cec.eu.int
Court of Justice of the European Communities	Marc SCHAUSS	DataProtectionOfficer@curia.eu.int
European Court of Auditors	Jan KILB	data-protection@eca.eu.int
European Economic and Social Committee	Elena FIERRO	data.protection@esc.eu.int
Committee of the Regions	Petra CANDELLIERr	data.protection@cor.eu.int
European Investment Bank	Jean-Philippe MINNAERT	DataProtectionOfficer@eib.org
European Ombudsman	Loïc JULIEN	dpo-euro-ombudsman@europarl.eu.int
European Central Bank	Wolfgang SOMMERFELD	dpo@ecb.int
European Anti-Fraud Office	Laraine L. LAUDATI	laraine.laudati@cec.eu.int
Translation Centre for the Bodies of the European Union	Benoît VITALE	data-protection@cdt.eu.int
Office for Harmonization in the Internal Market	<i>(to be nominated)</i>	DataProtectionOfficer@oami.eu.int
European Monitoring Centre on Racism and Xenophobia	Niraj NATHWANI	Niraj.Nathwani@eumc.eu.int
European Medicines Agency	Vincenzo SALVATORE	data.protection@emea.eu.int
Community Plant Variety Office	Martin EKVAD	ekvad@cpvo.eu.int
European Training Foundation	Romuald DELLI PAOLI	DataProtectionOfficer@etf.eu.int
European Network and Information Security Agency	Andreas MITRAKAS	dataprotection@enisa.eu.int

European Foundation for the Improvement of Living and Working Conditions	<i>(to be nominated)</i>	dataprotectionofficer@eurofound.eu.int
European Monitoring Centre for Drugs and Drug Addiction	Arne TVEDT	arne.tvedt@emcdda.eu.int
European Food Safety Authority	Claus REUNIS	claus.reunis@efsa.eu.int

1.3. Annex D — Prior-checking handling time per case and per institution

The following two charts illustrate the work of the EDPS and of the institutions and bodies by detailing the time spent on the prior checking cases. The first chart goes into details on each of the prior checking cases of 2005, and the second one summarizes the cases per institution and body.





The charts indicate the number of working days of the EDPS, the number of extension days required by the EDPS and the number of suspension days (time needed to receive information from the institution and bodies)³⁰. The following conclusions can be drawn:

- Number of working days of the EDPS per prior check

The number of working days of the EDPS is an average of 55.5 days per case, which can be considered satisfactory in that it is less than the stipulated two month period.

- Number of extension days for the EDPS

In 4 of the 34 prior checking cases (12 %) an extension period was requested, complying with Article 27 (4). This extension period has never exceeded one month and averages 28.5 days for those 4 files.

³⁰ Article 27 (4) of the Regulation is explained in paragraph 2.3.2.

- Number of suspension days

This is the amount of time taken to receive the additional information requested by the EDPS from the institutions and bodies. On average, the delay amounted to 30 days.

This number is not very relevant as it covers very extreme situations: for example, the shortest delay was 2 days, the longest 131 days. Ideally the institution or body should provide the information within a period of less than two months. On average, the chart clearly shows that a long period of time is sometimes required to answer the questions of the EDPS. Several reasons can be given for this. The first reason is the complexity of the case. A certain relation exists between the time needed by the EDPS (especially when an extension of delay has been granted) and the time needed for providing the further information requested. The second reason is the quality of notifications: the better the notification is, the shorter the further information period. A third reason is obviously the workload of the DPO or the controller of the institution or body concerned by the request of information.

These numbers and averages however are based on a limited number of cases as it is the first complete year of work of the EDPS. 2006 will determine whether these trends will continue. In addition, there will be more agencies sending processing operations subject to prior checking to the EDPS.

1.4. Annex E — List of prior-check opinions

Administrative enquiries and disciplinary proceedings — Court of Auditors

Opinion of 22 December 2005 on a notification for prior checking on internal administrative enquiries and disciplinary proceedings (Case 2005-316)

Administrative inquiries — European Central Bank

Opinion of 22 December 2005 on a notification for prior checking on internal administrative inquiries (Case 2005-290)

SYSPER 2 / CDR — Commission

Opinion of 15 December 2005 on a notification for prior checking on the ‘Sysper 2: staff appraisal — CDR’ (Case 2005-218)

Paid traineeships — European Economic and Social Committee

Opinion of 15 December 2005 on a notification for prior checking on the management of applications for paid traineeships (Case 2005-297)

Sick leave — Court of Justice

Opinion of 15 November 2005 on a notification for prior checking on ‘SUIVI: sick leave of translation directorate’ (Case 2004-279)

Online spontaneous applications — Committee of the Regions

Opinion of 28 October 2005 on a notification for prior checking on the management of online spontaneous applications (Case 2005-176)

Applications for traineeships — Committee of the Regions

Opinion of 27 October 2005 on a notification for prior checking on the management of applications for paid traineeships (Case 2005-214)

Applications for non-paid internship — Committee of the Regions

Opinion of 27 October 2005 on a notification for prior checking on the management of spontaneous applications for a non-paid internship (Case 2005-215)

‘SIC congés’ — Court of Justice

Opinion of 28 September 2005 on a notification for prior checking on the ‘SIC congés’ system (Case 2004-278)

Absences — European Central Bank

Opinion of 23 September 2005 on a notification for prior checking on recording the absences of ECB staff members unable to work because of illness or accident (Case 2004-277)

Double allocation — Court of Auditors

Opinion of 30 August 2005 on a notification for prior checking on double allocation (Case 2005-68)

Invalidity Committee — Court of Auditors

Opinion of 30 August 2005 on a notification for prior checking on the Invalidity Committee (Case 2005-119)

Periodical staff appraisal — OHIM

Opinion of 28 July 2005 on a notification for prior checking on periodical staff appraisal (Case 2004-293)

Disciplinary procedure — European Investment Bank

Opinion of 25 July 2005 on the notification for prior checking regarding data processing in the framework of the disciplinary procedure (Case 2005-102)

Harassment — Court of Auditors

Opinion of 20 July 2005 on the notification for prior checking on the issue of harassment (Case 2005-145)

Compass evaluation system — Court of Auditors

Opinion of 19 July 2005 on a notification for prior checking on ‘Compass’ (Case 2005-152)

‘Manager desktop’ — European Investment Bank

Opinion of 12 July 2004 on the notification for prior checking regarding the ‘Manager desktop’ file (Case 2004-307)

Assessment of work — Court of Justice

Opinion of 12 July 2004 on a notification for prior checking on the assessment of work (Case 2004-286)

‘Assmal’ — Council

Opinion of 4 July 2005 on a notification for prior checking on ‘Assmal application’ and ‘Assmal-Web’ (Cases 2004-246 and 2004-247)

Report at end of probationary period and staff report — Court of Justice

Opinion of 4 July 2005 on a notification for prior checking on ‘Personal files: report at end of probationary period and staff report’ (Case 2004-281)

Job applications — Court of Justice

Opinion of 4 July 2005 on a notification for prior checking relating to job applications and CVs of candidates (Case 2004-284)

Medical files — Court of Justice

Opinion of 17 June 2005 on the notification for prior checking relating to medical files (Case 2004-280)

Early retirement pension — Council

Opinion of 18 May 2005 on the notification for prior checking relating to the procedure ‘Selection of officials and temporary agents allowed early retirement pension’ (Case 2004-248)

‘IDOC’ — Commission

Opinion of 20 April 2005 on the notification for prior checking relating to internal administrative inquiries and disciplinary procedures within the European Commission (Case 2004-187)

Staff appraisal — European Central Bank

Opinion of 20 April 2005 on the notification for prior checking relating to the staff appraisal procedure (Case 2004-274)

Dignity at work — European Investment Bank

Opinion of 20 April 2005 on the notification for prior checking relating to the dignity at work policy (Case 2004-67)

Management of medical expenses — European Investment Bank

Opinion of 6 April 2005 on the notification for prior checking relating to the procedures for the administrative management of medical expenses (Case 2004-305)

Skills inventory — Council

Opinion of 4 April 2005 on the notification for prior checking relating to the skills inventory (Case 2004-319)

Disciplinary files — Parliament

Opinion of 21 March 2005 on the notification for prior checking relating to data processing in the context of disciplinary files (Case 2004-198)

‘Rapnot’ — Parliament

Opinion of 3 March 2005 on the notification for prior checking relating to the reports procedure and the Rapnot system (Case 2004-206)

‘EPES’ — Commission

Opinion of 4 February 2005 on the notification for prior checking relating to the appraisal of senior management staff (Case 2004-95)

Work rates — Commission

Opinion of 28 January 2005 on the notification for prior checking relating to work rates (‘Rythme de travail’) (Case 2004-96)

Selection procedure for temporary agents — OHIM

Opinion of 6 January 2005 on the notification for prior checking relating to an internal selection procedure for temporary agents (Case 2004-174)

1.5. Annex F — List of opinions on legislative proposals

Issued in 2005

Data protection in the third pillar

Opinion of 19 December 2005 on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final), OJ C 47, 25.2.2006, p. 27

Schengen information system (SIS II)

Opinion of 19 October 2005 on three proposals regarding the second-generation Schengen information system (SIS II) (COM(2005) 230 final, COM(2005) 236 final and COM(2005) 237 final)

Data retention

Opinion of 26 September 2005 on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), OJ C 298, 29.11.2005, p. 1

PNR Canada

Opinion of 15 June 2005 on the proposal for a Council decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of advance passenger information (API) / passenger name record (PNR) data, OJ C 218, 6.9.2005, p. 6

Visa information system (VIS)

Opinion of 23 March 2005 on the proposal for a regulation of the European Parliament and of the Council concerning the visa information system (VIS) and the exchange of data between Member States on short-stay visas, OJ C 181, 23.7.2005, p. 13

Criminal records

Opinion of 13 January 2005 on the proposal for a Council decision on the exchange of information from criminal records (COM(2004) 664 final of 13 October 2004), OJ C 58, 8.3.2005, p. 3

Prepared in 2005; issued in January 2006

Access to VIS by authorities responsible for internal security

Opinion of 20 January 2006 on the proposal for a Council decision concerning access for consultation of the visa information system (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final)

1.6. Annex G — Composition of the EDPS Secretariat

Sectors under the direct authority of the EDPS and Assistant EDPS

— Supervision

Sophie Louveaux
Administrator

Sylvie Longrée
Supervision Assistant

Eva Dimovne Keresztes
Administrator

Kim Thien Lê
Secretary

Maria Veronica Perez Asinari
Administrator

Vasilios Sotiropoulos
Trainee (Oct. 2005 to Feb. 2006)

Endre Szabo
National Expert

Zoi Talidou
Trainee (Oct. 2005 to Feb. 2006)

Delphine Harou (*)
Supervision Assistant

Anna Vuori
Trainee (Oct. 2005 to Feb 2006)

Xanthi KAPSOSIDERI
Supervision Assistant

(*) Information team.

— **Policy and Information**

Hielke Hijmans

Administrator

Per Sjönell (*)

Administrator / Press Officer

Laurent Beslay

Administrator

Martine Blondeau (*)

Documentation Assistant

Bénédicte Havelange

Administrator

Andrea Beach

Secretary

Alfonso Scirocco

Administrator

Herke Kranenborg

Trainee (Jan. to Mar. 2006)

Personnel/Budget/Administration Unit

Monique Leens-Ferrando

Head of Unit

Anne Levêcque

Human Resources Secretary

Giuseppina Lauritano

Administrator / Statutory Questions and Audit

Alexis Fiorentino

Accounting Clerk

Vittorio Mastrojeni

Human Resources Assistant

Annex H — List of administrative agreements and decisions

1.6.1. 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 and Employment, Social Affairs and Equal Opportunities DG)
- Service-level agreement with the Council
- Service-level agreement with the European Administrative School (EAS)

1.6.2. 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 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 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

European Commission

XXX

Luxembourg: Office for Official Publications of the European Communities

2005 — xx pp. — 21 × 29.7 cm

ISBN 92-95030-00-1

SALES AND SUBSCRIPTIONS

Publications for sale produced by the Office for Official Publications of the European Communities are available from our sales agents throughout the world.

You can find the list of sales agents on the Publications Office website (<http://publications.eu.int>) or you can apply for it by fax (352) 29 29-42758.

Contact the sales agent of your choice and place your order.



Annual Report 2005

Summary

Postal address: rue Wiertz, 60 — B-1047 Brussels

Office: rue Montoyer, 63, Brussels, Belgium

E-mail: edps@edps.eu.int — Website: www.edps.eu.int

Tel. (32-2) 283 19 00 — Fax (32-2) 283 19 50

Annual Report 2005

Summary ¹

Introduction

This is a summary of the second annual report of the European Data Protection Supervisor (EDPS), an independent authority set up to ensure that the European Community institutions and bodies respect their obligations when it comes to the fundamental right to protection of personal data.

While 2004 was the first year of activity, during which a new institution was literally built up (including finding appropriate office space and the first phases of recruitment), the second annual report covers a year of consolidation. The three main roles of the EDPS laid down in Regulation (EC) No 45/2001² - supervision, consultation and cooperation – were further refined and broadly recognized by those concerned. A press service was established and efforts were devoted to developing external communications. The size of the authority grew moderately with new recruitments and temporary support from the first trainees.

It is important to emphasize that **more and more EU policies depend on the lawful processing of personal data**. Many public or private activities in a modern society nowadays generate personal data or use such data as input. This is naturally also true for the European institutions and bodies in their administrative and policy making roles, as well as for the implementation of their policy agenda. **Effective protection of personal data**, as a fundamental value underlying EU policies, should be seen as **a condition for their success**. The EDPS will continue to act in this general spirit and expects a positive response in return.

¹ The full text of the Annual Report 2005 and all of the reference documents can be downloaded from our website – www.edps.eu.int. Printed copies can also be ordered from the secretariat: edps@edps.eu.int.

² OJ L 8, 12.1.2001, p. 1

Supervision

The EDPS's supervisory role is to monitor and ensure that Community institutions and bodies comply with existing legal safeguards whenever they process personal data. In that sense, the EDPS complements the national data protection authorities that supervise the processing within their respective Member States. The major developments of 2005 in the context of improving the data protection culture of the institutions and bodies were:

Firstly, efforts were devoted to the further development of the network of **Data Protection Officers** (DPOs) of institutions and bodies. These officers have the task of ensuring in an independent manner the internal application of Regulation 45/2001. In November 2005, a position paper was issued on their role in ensuring effective compliance with the Regulation. The paper was sent to the heads of the EU administration and it underlines the fact that the DPOs are a strategic partner for the EDPS. One of the key messages is that all bodies need to appoint a DPO as a vital first step on their way towards complying with their data protection obligations. A second key message is that DPOs must be notified more adequately of personal data processing within their institution or body and that they notify to the EDPS those processing operations that entail specific risks for the people concerned and therefore need to be prior checked.

Secondly, considerable resources were allocated to **prior checking** those processing operations that are likely to present specific risks. Although this task was typically designed to deal with new processing operations before they start, most prior checks have so far been 'ex post' as many of the existing systems were launched before the EDPS started its activities or before the Regulation entered into effect.

In 2005, 34 opinions were issued on prior checking cases, 30 of which were on existing systems of various institutions and bodies. Other cases were consultations about the need for prior checking, or cases found not to be subject to prior checking which still gave reason for comments. The EDPS has defined a number of thematic priorities, which guide the prior checking, notably medical files, staff appraisal, disciplinary procedures, social services and e-monitoring. At the end of 2005, 29 notifications were in process and many more are expected in the near future. The institutions and bodies have been encouraged to submit their notifications for prior checking by spring 2007 at the latest.

Thirdly, the EDPS received some 27 **complaints** last year, although only 5 of them were declared admissible and further examined. In practice, a large majority of complaints received fall outside the EDPS's area of competence. In such cases, the complainant is informed in a general way and, if possible, advised on a more appropriate alternative. With respect to the handling of complaints within his competence, the EDPS has been in contact with the European Ombudsman to examine a potential scope for collaboration in the near future.

Fourthly, considerable efforts were invested in the elaboration of a background paper on how the two fundamental rights **public access to documents** and **data protection** relate in the context of the EU institutions and bodies. Work on another paper, concerning the use of **electronic communications** has begun, and the paper will be published by mid-2006.

Finally, a number of activities relating to the shared supervision of **Eurodac** (the finger print system used for asylum procedures throughout the EU) were prepared. The EDPS is the supervisory authority of the central unit, while the national data protection authorities are responsible for supervising the use of Eurodac in their respective Member States. The EDPS was globally satisfied with the findings of the first phase of his inspections.

Consultation

The EDPS's consultative role is to advise Community institutions and bodies on all matters relating to the protection of personal data, and especially on proposals for legislation that have an impact on data protection.

A **paper on the advisory role**, presented in March 2005, lays down the policy. It emphasizes that the advisory task has a wide scope, which was subsequently confirmed by the Court of Justice. The policy paper also sets out the substantive approach towards proposals for legislation that have a data protection impact, as well as the procedural role in the different stages of the legislative process. The paper was well received and the European Commission is making good use of the availability of the EDPS to make informal comments on a draft proposal before it is submitted for formal consultation. All formal opinions are published and most often presented to a relevant committee in the European Parliament and/or the competent working party of the Council, and systematically followed throughout the legislative process.

The EDPS issued six formal **opinions** in 2005 which clearly reflect the relevant subjects on the policy agenda of the Commission, the Parliament and the Council. The most significant were:

- the exchange of personal data in the 'third pillar' of the EU (police and judicial cooperation in criminal matters);
- the development of large scale information systems, such as the Visa information system (VIS) and the second generation of the Schengen information system (SIS II); and
- the highly controversial subject of the mandatory retention of data on electronic communications for access by law enforcement authorities.

The EDPS also advises on **administrative measures**, and more in particular on implementing rules of institutions and bodies in the area of data protection. This provides an important opportunity to influence, in a more structural fashion, the way in which data protection policies are implemented. Advice was given on the specific implementing rules concerning the role of DPOs.

The EDPS also, for the first time, made use of the possibility to **intervene in cases** which raise important questions of data protection **before the Court of Justice**. The cases concerned the transfer of PNR-data on airline passengers to the United States, and the EDPS intervened in support of the conclusions of the Parliament, which seeks to annul the related decisions of the Commission and the Council.

Cooperation

The EDPS's cooperative role includes working together 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.

A very important platform for cooperation with national supervisory authorities is the **Article 29 Working Party**, established by Directive 95/46/EC to advise the Commission and to develop harmonised data protection policies, of which the EDPS is a full member. A certain number of important proposals for legislation were covered by the EDPS and the Working Party in separate opinions. In these cases, the EDPS has welcomed the general support of national colleagues as well as additional comments which can lead to better data protection.

Cooperation with **supervisory bodies in the 'third pillar'** (i.e. supervisory bodies for Schengen, Customs, Europol and Eurojust - usually made up of representatives of national supervisory authorities) has concentrated to a large extent on the preparation of common positions with a view to the development of a much needed general framework for data protection in the third pillar of the EU. Discussions have also taken place around a new system of supervision with regard to SIS II which will build on a close cooperation between national supervisory authorities and the EDPS.

The EDPS has cooperated actively in the context of the **European and International Conferences** of Data Protection Commissioners, and has chaired different sessions.

In September 2005, in cooperation with Council of Europe and OECD, the EDPS hosted a workshop on data protection in **international organisations**. Often exempted from national laws, including laws on data protection, international organisations should nevertheless subscribe to the universal principles on data protection, as they also process sensitive data in many cases.

External communications

In 2005, specific attention was paid to the development of an **information strategy** that can give adequate support to the strategic roles of the EDPS. Raising awareness about data protection generally, and about the roles and activities of the EDPS more specifically, is an important condition for effective supervision, consultation and cooperation. The information strategy has distinguished target groups in relation to the different roles:

- Supervision: data subjects, notably EU staff (as the individuals whose data are processed) and DPOs and controllers, as responsible for the processing systems.
- Consultation: the European legislator; the Commission, the Parliament and the Council, focusing on specific DGs, committees and working groups.
- Cooperation: the Article 29 Working Party and other relevant forums for cooperation, such as in the joint supervisory bodies in the third pillar, and the European and the International Data Protection Conferences.

The EDPS has also invested in an enhancement of **information and communication tools**. A general information campaign in all EU institutions and bodies, and in all Member States, was followed up in 2005 by the introduction of a press service, a regular newsletter, the development of a new logo and house style, and will soon be completed by the introduction of a new website, which will be the most important tool of communication for the EDPS.

Resources

The budget authorities provided the **budgetary means** for consolidation and limited growth of the organisation, taking into consideration the need to address urgent tasks in supervision and consultation on data protection in most institutions and bodies. Major attention was devoted to the development of **human resources** and important results were achieved, both in the general area of recruitment and in special programs for traineeships and secondment of national experts.

In this context, it is difficult to overemphasise the importance of the **administrative agreement**, concluded in 2004 with the Commission, the Parliament and the Council, which has enabled the EDPS to benefit from outside support where appropriate, and to invest most resources in primary activities. A continuation of this agreement after the initial three years is therefore essential.

Perspectives

The Commission is promoting a European Information Society, based on innovation, creativity and inclusion. This society will rely on three major **technological trends**: an almost unlimited bandwidth, an endless storage capacity and ubiquitous network connections, which will naturally have implications for data protection. Data protection will be put in a new context: new forms of processing like Web Services and an erosion of the traditional technological barriers (power limitations, limited transmission range, isolated data, etc). This is well illustrated by the growing use of RFID tags and the massive development of communication networks which have great impact:

- all tagged objects become a collector of personal data;
- smart objects, carried by individuals, are always 'present' and 'active';
- an enormous amount of stored data is continuously fed with new data.

New and emerging technologies that will have an impact on data protection include:

- **RFID**: a promising and challenging technology which will constitute key elements of the so-called Ambient intelligence environments.
- **Ambient intelligence environments**: privacy and data protection requirements should be part of their design, to allow for domestication and a subsequent wide acceptance.
- **Identity management systems**: a (partly biometrics based) key element of emerging e-government services which will require proper standards.
- **Use of biometrics**: common requirements based on their inherently sensitive nature should be laid down.

A number of new **developments in policy and legislation** can also be noted, such as a focus on activities in the area of police and judicial cooperation and a general trend to increase exchanges of data between law enforcement authorities of EU Member States. Another trend concerns extending the investigative powers of law enforcement agencies (frequently including Europol) by granting them access to databases which are not originally developed for law enforcement purposes. This confirms the desirability of a comprehensive legal framework for the protection of personal data in the third pillar, independently from the approval of the proposal on the availability principle, as stated in the EDPS opinion on data protection in the third pillar.

At the end of 2005, the Commission started the process for a review of the regulatory framework for electronic communications and services, including the review of Directive 2002/58, which will be followed closely by the EDPS.

It is clear that the agenda of the EDPS as a legislative advisor is largely determined by the work programme of the Commission. It is quite likely that the mid and long term focus will partially shift towards:

- the theme 'prosperity', where the EDPS will follow further initiatives towards the development of a European Information Society.
- the theme 'security', where the EDPS will follow developments in relation to technological developments such as biometrics and the growing pressures on public and private controllers of databases to allow access for law enforcement purposes. In this context, the Commission presented as a key initiative the access by police forces to databases for external border control.

Objectives for 2006

With this in view, the EDPS priorities for 2006 are:

- Support of the DPO network, including bilateral evaluations of progress in notifications, aiming for notifications of existing operations to be completed, latest by spring 2007.
- Continue prior checking, finalising those that concern existing processing operations in the thematic priorities.
- E-monitoring and traffic data: issue guidelines on processing of personal data related to the use of electronic communication networks.
- Personal files on staff: issue guidelines on content and conservation periods.
- Transfer to third countries: issue guidelines on personal data transfers to third countries, international organisations and European bodies outside the scope of Regulation 45/2001 and Directive 95/46/EC.

-
- Supervision of Eurodac: an in-depth security audit of Eurodac's central data base.
- Advice on legislative proposals: consolidate and further develop the role of the EDPS and issue opinions on various subjects.
- Interventions in Court cases: consider intervention in cases raising data protection issues.
- Second version of website: will be launched by mid-2006.
- Development of resources: seek a prolongation of the present administrative agreement with Commission, Parliament and Council, and adequate enlargement of available office space to accommodate current needs and expected increases in staff.