NE-AC-07-001-EN-N

Ninth Annual Report

of the Article 29 Working Party on

Data Protection

EUROPEAN COMMISSION

Ninth Annual Report

EUROPEAN COMMISSION

of the Article 29 Working Party on **Data Protection**

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on the Protection of personal data. Its tasks are laid down in Article 30 of Directive 95/46/EC and can be summarized as follows:

- To provide expert opinion from member state level to the Commission on questions of data protection.
- To promote the uniform application of the general principles of the Directive in all Member States through co-operation between data protection supervisory authorities.
- To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data.
- To make 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.

ISBN 978-92-79-04789-3

Ninth Annual Report

on the situation regarding the protection of individuals with the regard to the processing of personal data and privacy in the European Union and in third countries

Covering the year 2005

Adopted on 14 June 2006

This report was produced by Article 29 Working Party on data protection.
It does not necessarily reflect the opinions and views of the European Commission nor is it bound by its conclusions.
This report is also available in German and French. It can be downloaded from the 'Data Protection' section on the website of the European Commission's Directorate-General Justice, Freedom and Security www.ec.europa.eu/justice_home/fsj/privacy

TABLE OF CONTENTS

INTRODUCTION BY THE CHAIRMAN OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY

In 2005 notably three elements have dominated the data protection scene in Europe:

- The rapid development of information technology makes it necessary to check and to adapt the instruments of data protection.
- It is in the EU citizens' interest to take further legal and practical measures to achieve harmonisation of data protection on a high level.
- The ongoing quest of Europe for the right answers to international threats to security must not result in an unreasonable and unacceptable encroachment upon civil liberties and, in particular, upon data protection.

In the past decade, the European concept of data protection has emerged as a globally attractive model. This model has to constantly prove its usefulness; otherwise, it will risk losing its attractiveness. It has to be open to innovations and it has to take the latest technological, economical and social developments into account. Its focus has to be the EU Member States' more than 450 million citizens, whose rights and interests are to be guaranteed.

Since its foundation in 1995, the Article 29 Working Party has assessed new technological developments at an early stage and it has influenced both their design and application with respect to data protection. In the year covered by this report, the Working Party paid particular attention to Radio Frequency Identification (RFID), which is used already now in many areas and which will steadily gain importance for the individual's privacy. After intensive preparation by a sub group, and on the basis of results of a public online-consultation, the Working Party has brought forth some essential guidelines (WP 105 and WP 111).

One of the results shows that the concept of "personal data" contained in Directive 95/46/EC and the issue of possible anonymisation and identifiability require further in-depth studies. Notably, it has to be found out whether the current regulations take sufficiently into account the fact that, when using RFIDs as numbering systems for goods during their life cycle, phases of the involved persons' anonymity and identifiability follow in a rapid succession. It is questionable how far the directive covers these dynamic processes and changes of context of certain data in its life cycle. Therefore, the Working Party included this issue in its work programme of the following year.

Other important technological topics were the use of localisation data provided by telecommunications and value added-services (WP 115), safeguards concerning biometric features in passports (WP 112) as well as the European Visa Information System (VIS) (WP 110). It has also to be mentioned that due to the combination of biometric features and progressing technologies regarding storage, transmission and software (pattern recognition), qualitatively new risks arise for the right of informational self-determination which have to be counteracted by adequate security measures. Moreover, the Working Party dealt with data protection implications when intellectual property rights are being exercised by currently available means (WP 104).

One of the Article 29 Working Party's strategic aims is not only to harmonise and to push forward the data protection regulatory framework on a European level, but also to pay considerable attention to the practical implementation which must not fall behind the programme. In the EU citizens' life, data protection should be a reality present and sizable at any given time. In pursuit of this aim, the Working Party managed to lay down two important milestones in the last year. The first one concerns binding corporate rules for data protection applicable by companies dealing in an international environment. With a view to ensuring an adequate data protection level while transferring personal data to third countries, the members of the Working Party agreed that this instrument should be as strongly accepted as the contractual clauses which are mentioned explicitly by the Directive. As a result of intensive preparations and deliberations with the business sector, the Working Party has compiled a catalogue of requirements that these international binding corporate rules have to comply with.

The Directive provides that such safeguards have to be evaluated under the national law of the Member States in which they are to be applied. Up to now, mutual acceptance is not foreseen. However, in order to find solutions with a view to European harmonisation, the Working Party agreed on a co-operation procedure facilitating the adoption of binding corporate rules across Europe. To achieve this goal, the Working Party focuses on the approach where a company negotiates only with one supervisory authority which coordinates on its part a common position with the other supervisory authorities in charge. Some international companies have already chosen this method; the coordinating procedures between the supervisory authorities of the respective Member States are still under discussion.

One project of a particularly practical, but also strategic dimension is the envisioned joint European-wide data enforcement action. The data protection authorities intend to increase the effect of their investigation activities by auditing certain areas in a clearly defined temporal and subject-related framework. This enables them not only to recognise differences in the practical implementation of the Data Protection Directive and of the national data protection law, but also to jointly work out and to implement best practises based on comprehensive experience. In order to achieve this objective, the Working Party has elaborated principles for a joint procedure. The first joint audit will take place in the course of 2006 in the area of private health insurance companies. By conducting this exercise, the data protection authorities want to learn more from each other, and at the same time, they regard it as an important contribution to the harmonisation of their practical activities.

In autumn 2005, on the basis of an agreement[1] reached between the EU and the USA, representatives of the Article 29 Working Party and representatives of the Commission jointly reviewed the American border protection authorities' practice regarding the processing of air passenger data (PNR). By this exercise, the Article 29 Working Party has made an important contribution in the field of practical implementation of data protection. The review of the way how US authorities deal with PNR data with the involvement of the independent data protection authorities underlines the significance Europe attaches, also in the international context, to the respect of privacy as one of the central civil rights. The visit resulted in a number of improvements. The Working Party dealt furthermore with the transfer of air passenger data to Canada and to Australia, as respective agreements were being prepared by the European Commission.

[1] The PNR agreement was annulled by the European Court of Justice on 30 May 2006

Finally, in the year covered by the report, the Working Party participated in an American-European review of the Safe Harbor scheme[2] after the European Commission had carried out an evaluation in 2004. Both sides, including the representatives of the business sector taking part in Safe Harbor, considered this review a success. They envision to further improve the Safe Harbor system and to open it up to business sectors not yet participating due to pertinent American legislation.

In the year covered by the report, the performance of the Working Party was also dominated by discussions on the issue how to protect privacy vis-à-vis permanent terrorist threats. Pending initiatives by the Council and the Commission gave the Working Party repeatedly cause to voice its opinion on respective proposals. In this context, the discussion on obliging electronic communications service providers to collect and retain traffic data at a large scale was of particular importance. It is one of the principles of a free country that a government only intrudes into the citizens' privacy if there is a concrete reason warranting such a measure. In this case, information available at companies and from individuals is principally accessible to governmental law enforcement and security authorities. The regulations adopted by Parliament and the Council as a result of their agreement are, however, of a qualitatively, absolutely different character: They oblige electronic communications service providers to retain data, which would otherwise not be needed, and to keep them accessible for a long period, with the intention of providing governmental agencies with a major data basis in case of necessity. In other words, the issue is no longer the intervention in individual cases, but a preventive surveillance structure.

The representatives of the European data protection scene have repeatedly voiced their position. They pointed to the requirements of the European Convention on Human Rights, which does not allow an unfounded systematic, preventive supervision. They have – without success – demanded to examine alternative approaches, which other governments regard as sufficient, in particular the 'quick-freeze' procedure which is being successfully applied in the USA.

Against the background of the decision taken by the European organisations, the data protection authorities co-operating in the Working Party will strive to harness the remaining free space left for transposing the Directive into national law to guarantee an effective protection of privacy and of basic rights. Furthermore, they will closely monitor the results of preventive traffic data retention. Finally, they voiced their willingness to participate in the evaluation of the regulation. The guidelines applying to all persons involved have to be, notably concerning terrorist threats, to preserve the fundamental principles of proportionality, clarity, and transparency.

The Article 29 Working Party will also strive in the future to reinforce data protection for EU citizens and to adapt the required instruments to the changing framework conditions and the challenges ahead. At the same time, an effective privacy protection is an indispensable element of a democratic information and knowledge society.

Peter Schaar, Chairman of the Article 29 Data Protection Working Party

[2] http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm

[3] All documents adopted by the Art. 29 Data Protection Working Party can be found under http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm

Chapter One

Issues Addressed by the Article 29 Data Protection Working Party[3]

1.1. TRANSFER OF DATA TO THIRD COUNTRIES

1.1.1. Binding Corporate Rules

Working Document Setting Forth a Co-operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting from "Binding Corporate Rules"[4]

This document should be referred to if a corporate group is interested in submitting draft binding corporate rules (BCRs) for the approval of several data protection authorities and therefore proposing a Data Protection Authority (DPA) as the lead authority for the co-operation procedure; it should also justify the selection of the lead authority on the basis of relevant criteria as well as all the whole procedure to be followed.

Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules[5]

Since the participation of data protection authorities in the approval of binding corporate rules is entirely voluntary, the decision to participate can be made on a case-by-case basis. This document establishes a model checklist to assist a group of companies when it applies for approval of its binding corporate rules and in particular to help demonstrate how the group complies with the WP74 document which sets out the requirements for the binding corporate rules.

1.1.2. Article 26(1) of Directive 95/46/EC

Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995[6]

This working document aims to provide guidance as to how Article 26(1) of Directive 95/46 should be understood and applied by data controllers intending to initiate data transfers to countries which do not ensure an adequate level of protection, in the sense of Article 25 of the said Directive. This document will be useful to clarify how data controllers may, and sometimes should make use of the derogations of Article 26(1). The Working Party (WP) considers this document as an essential element of its policy on data transfers to third countries.

1.1.3. Canada

Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines[7]

The present Opinion is issued in the light of the Commitments (document issued by the Commission, containing the Commitments by the Canada Border Services Agency in relation to the application of its PNR Program). It is also issued with reference to the level of protection ensured by Canada once airlines have transmitted API and PNR data relating to their passengers and crewmembers to the CBSA, on the basis of the Canadian law and the Commitments. The WP assumes that Canada ensures an adequate level of protection within the meaning of Article 25(6) of the Directive.

4 WP 107
5 WP 108
6 WP 114
7 WP 103

1.2. ENHANCEMENT OF COMPLIANCE WITH THE DATA PROTECTION DIRECTIVE

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 the data protection officers in the European Union[8]

This report identifies best practices as regards the duty of notification in the Member States including the role of data protection officials. It also explores a possible system of simplification for organisations with more than one establishment in the EU, and it issues some recommendations which the European Commission is invited to take into account if further harmonisation attempts were envisaged for the future. This report should be regarded as a first contribution for a better understanding of the role of notification duties and of data protection officials in the data protection system existing in the European Union and as a first step in the progress of providing further harmonisation and simplification to notification duties in the Community.

1.3. INTERNET, TELECOMMUNICATIONS AND NEW TECHNOLOGIES

Opinion 4/2005 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 (CON(2005)438 final of 21.09.2005)[9]

In this Opinion several considerations have been made such as traffic data retention interferes with the inviolable, fundamental right to confidential communications; any restriction on this fundamental right must be based on a pressing need, should only be allowed in exceptional cases and be the subject of adequate safeguards. This Opinion sets out twenty specific safeguards to be envisaged with particular regard to the requirements applying to recipients and further processing, the need for authorisations and controls, the measures applying to service providers also in terms of security and logical separation of the data, determination of the data categories involved and their updating, and the need to rule our contents data.

Opinion 5/2005 on the use of location data with a view to providing value-added services[10]

The WP notes that issues related to the use of location data are very topical. Such data are defined as "any data processed in an electronic communications network, indication the geographic position of the terminal equipment of a user of a publicly available electronic communications service" (Article 2 of Directive 2002/58/EC). With this Opinion the WP points out that, when processing personal data, the various parties involved in providing a value-added service based on the use of location data, whether they are electronic communications operators who process location data or third parties providing the valued-added service on the basis of location data sent to them by operators, must comply with their obligations under data protection legislation on protecting personal data.

[8] WP 106
[9] WP 113
[10] WP 115

1.4. SCHENGEN/VISA/FREE MOVEMENT OF PERSONS

Opinion 2/2005 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 (COM (2004) 835 final)[11]

In this Opinion several considerations have been made regarding the project of setting up a central database and a system of exchange of information concerning short-stay visas which raises important questions for fundamental rights and freedoms of individuals and in particular their right to privacy as it will lead to a massive collection and processing of personal and biometric data, their storage in a centralised database to large scale exchanges of information concerning a huge number of persons. This Opinion also states the potential risks of such a project and stresses the importance of ensuring proper respect for the principles of data protection. The question of necessity and proportionality of such a large database, in particular with respect to the choice of integration of biometric data held in the system has been also raised. The WP proposes the amendment of this Proposal in the light of the remarks stated in this Opinion.

Opinion 3/2005 on implementing the Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States[12]

Following the work carried out in 2004[13], the Opinion of the Working Party of 30 September 2005, stresses the position already expressed by the Working Party with regard to the use of biometric indicators in passports and travel documents issued by Member States, as provided in Regulation 2252/2004.[14] The Working Party reminds its long-standing position about the processing of biometric indicators and states that the implementation of biometric features in passports and travel documents raises major technical, ethical and legal questions. In particular the Working Party points out that the use of biometric indicators effective safeguards have to be implemented to avoid inherent risks posed by biometrics; it also calls for restricting the use of biometric indicators in passports and travel documents for verification purposes and for guarantees that only competent authorities would be able to have access to these data stored in the chip.

Opinion 6/2005 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)[15]

In this Opinion, adopted on 25 November 2005, the Working Party considers that several aspects of the legislative package presented by the European Commission raise concern from the perspective of compliance with data protection principles. This Opinion joins

[11] WP 110
[12] WP 112
[13] See Eighth Report, section 1.4
[14] OJ n° L 385, 29.12.2004 p. 1
[15] WP 116

the opinions delivered by the EDPS[16] and the Joint Supervisory Authority of Schengen.[17] The Working Party stresses that the new regime for the protection of personal data proposes should be at least equal to the existing level provided by the current Schengen Information System.

In its opinion the Working Party addresses in particular questions relating to the objective and purpose of the SIS II; it considers that granting access to the system to new categories of authorities goes beyond the purposes limitation criterion and should be avoided, the provisions relating to the interlinking of alerts entered in the system require detailed safeguards on the use of such link and the need of avoiding the creation of new access rights in favour of authorities in respect of information to which they are not entitled. National copies should also be avoided as they do not appear to be justified, resulting in a multiplication of access points. The Working Party also raises concern about the processing of biometric indicators in the system. In accordance with its constant position on this topic, the Working Party insists on the fact that using biometric indicators should be strictly limited and with appropriate safeguards. Searches bases on biometrics should be ruled out. The length of the period for the retention of personal data processed. Finally, and with respect to the supervision of the system, the Working Party asks for clear regulations on the role and the obligations of the supervisory authorities involved in order to better structure and enhance the co-operation between national supervisory authorities and the EDPS.

1.5. RFID

Working document on data protection issues related to RFID technology[18]

With this Opinion the WP express its concerns on the possibility for some applications of RFID technology to violate human dignity as well as data protection rights. In particular, concerns arise about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens. The WP is committed to continue monitoring the technological developments in this field in collaboration with interested parties. Furthermore, depending on the evolution of the RFID technology and its applications, at a later stage the WP may decide to focus in detail on specific areas/applications by providing additional guidance for specific applications.

Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues related to RFID technology[19]

Following the adoption of the above-mentioned document, the WP decided to put it up for public consultation. This document contains the summary of the main comments and some conclusions, which it would be useful to share it with stakeholders in general.

[16] Opinion of the EDPS of 19.10.2005
[17] Opinion of 6 October 2005
[18] WP 105
[19] WP 111

1.6. INTELLECTUAL PROPERTY RIGHTS

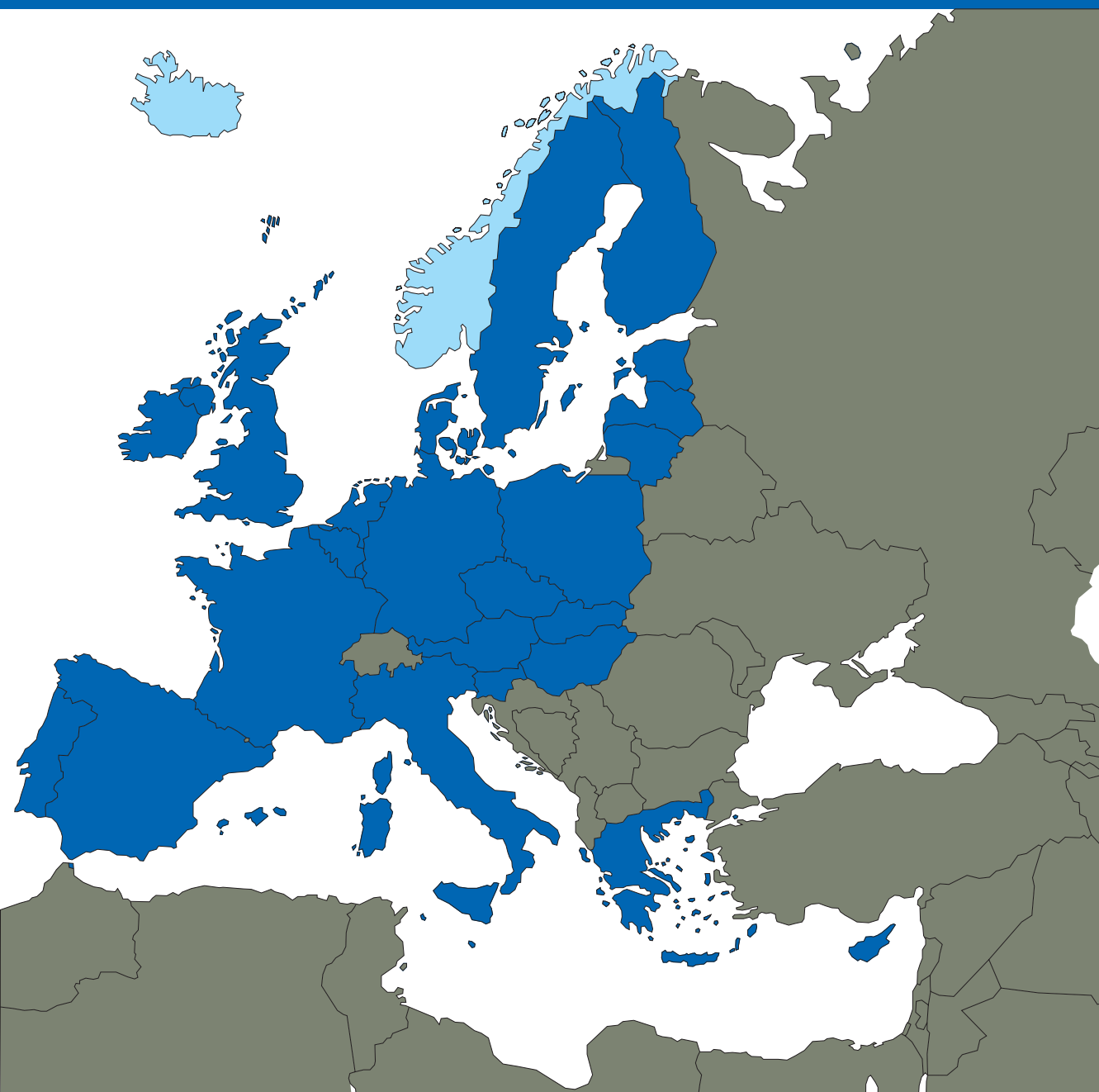
Working document on data protection issues related to intellectual property rights[20]

The WP notes that the increasing exchange of information linked to the development of the Internet touches more and more the delicate question of control over copyright protected information. This document intends to recall not only the main legal principles to be complied with by copyright holders in the exercise of the rights, but also by other actors involved more specifically in the digital management sphere, such as the industry and service providers offering digital rights management technology. With this document the WP calls for a development of technical tools offering privacy compliant properties, and more generally for a transparent and limited used of unique identifiers, with a choice option for the user.

[20] WP 104

Chapter Two

Main Developments in Member States



Austria

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

In the aftermath of the tsunami disaster in December 2004, more detailed provisions for processing personal data (including sensitive data) in case of a catastrophe were implemented in the Austrian Data Protection Act 2000 (DP Act 2000). Thus, public authorities and aid organisations may lawfully process data in case of a catastrophe as far as this is necessary to provide assistance to people directly affected by the catastrophe or to locate and to identify missing and deceased persons and to furnish information to family members. It is permitted to operate and participate in a joint information system when necessary to cope effectively with a catastrophe. Within the scope of the aforementioned objectives, data transfers to third countries are also admissible including participation in a joint information system with third country participants. However, forwarding police records or sensitive data into such a joint information system is only permitted when tangible indications for the death of the missing person exist. Criminally relevant information may not be forwarded unless this is absolutely necessary for identification purposes in a particular case. Information (e.g. DNA-data for identification purposes) about family members may only be transferred in a pseudonymous way (cf. Federal Law Gazette Part I No. 13/2005).

Furthermore, amendments of the Telecommunication Act 2003 (TC Act 2003) became necessary in order to render it more compatible with the Directive on Privacy and Electronic Communications (Directive 2002/58/EC). The said Directive includes all natural persons without any differentiations. Section 107 TC Act 2003, however, provided that it should not be permissible to send e-mails – without obtaining prior consent – "to consumers for direct marketing purposes". Thus, it was not necessary to obtain prior consent from entrepreneurs. This distinction was incompatible with the wording of the Directive 2002/58/EC and had to be removed. Additionally, a new paragraph was introduced in Section 107 providing for the possibility to initially refuse the use of electronic contact details for direct marketing purposes.

B. Major case law

A privately owned, officially recognised detox centre intended to participate in a publicly funded research project. The aim of this project was to evaluate a reprieve system for drug addicts who had submitted themselves to a detoxification therapy. This reprieve system, called "therapy instead of penalty", was introduced into the Austrian legal system only a couple of years ago and its effects should be reviewed now.

In this context, the scientific project supervisor of the detox centre applied for permission to use the personal data of drug addicts who submitted themselves to a detoxification therapy.

According to Section 46 para. 3 Austrian DP Act 2000, permission for the use of personal data for purposes of scientific research or statistics may be granted if the following three conditions are met: consent of the data subject is actually impossible to obtain or the effort would otherwise be unreasonable, there is a public interest in the use of data for which a permit is sought and the scientific

qualification of the applicant has satisfactorily been demonstrated.

In the present case, it was intended to use medical data (about the results of the detoxification therapy) of persons who had been criminally convicted before treatment.

The Austrian DPA rejected the application on grounds that consent should be obtained as it cannot be plainly assumed that this would constitute unreasonable efforts, especially not when dealing with two kinds of extremely sensitive data.

In a case of "video-surveillance" for the sake of documenting the frequency of air traffic with high noise level the Austrian DPA rejected the complaint of a pilot on the grounds that image data falls outside the scope of the data protection regime whenever it is recorded clearly without the intention of identifying recorded persons. Furthermore, it was concluded that an analogue video tape recording with one single, hand-operated camera in conjunction with manually written records is not a "personal data filing system". Analogue video tape recording is not done "by automated means" as opposed to digital recording. Such documentation is not a structured set of personal data which is accessible according to specific criteria.

The Austrian DPA received a notification regarding video surveillance on public transportation for the purpose of preventing vandalism and increasing the protection of employees and passengers. The technical structure of the system allows digital recordings up to 48 hours. Recordings are only analysed in case somebody pressed the emergency button or in case damage due to vandalism was detected. In either case, the data medium is disassembled and delivered to specially trained employees to analyse the recordings.

The Austrian DPA concluded that video surveillance is subject to prior notification as such recordings reveal data about ethnic origin and potentially also health related data and in the case under consideration, presumably also criminally relevant data.

The Austrian DPS concluded, furthermore, that video surveillance constitutes a new type of data application which still needs to prove that it is an adequate means for preventing vandalism and increasing security. Any interference with the right of privacy must, however, be adequate and necessary to achieve the specified purpose. Due to insufficient documentation of this issue, the Austrian DPA issued only preliminary permission and imposed special requirements (i.e. detailed documentation of all incidents leading to an analysis of the recordings).

The Austrian DPA received a complaint by an Israeli citizen against the French Ministry of Internal Affairs on the basis of Article 110 ("right of deletion") of the Convention on the Implementation of the Schengen Agreement.

In the preliminary events leading to this complaint, the complainant attempted to enter French territory. However, the French border police decided to refuse the entry on the grounds that his presence on the French territory posed a threat to public security. Consequently, his data was stored in the national (French) section of the Schengen Information System (N.SIS). This alert had been thereafter transmitted to the national sections of all Member States, including the Austrian N.SIS.

The complainant contested this decision in France with the result that the decision of the French border police was annulled by a French administrative court. However, the alert was not deleted and when the complainant applied for a visa in the Austrian Embassy in Tel Aviv, the visa was refused.

Based on the facts, the Austrian DPA decided that the French Ministry for Internal Affairs was obliged to delete the alert from the national French section of the Schengen Information System; the competence of the Austrian DPA is based on Article 111 para. 1 leg. cit., saying that "any person may, in the territory of each contracting party, bring before the courts or the authority competent under national law an action to correct, delete or obtain information or to obtain compensation in connection with an alert involving them".

C. Major specific issues

In the first half of 2005, Austrian courts issued a number of Decisions regarding the duty of internet service providers to disclose the identity of file sharing users. The main question in this context was whether or not a "dynamic" IP address constitutes "traffic data" according to Article 2(b) and recital 15 Directive 2002/58/EC with the consequence that it may only be disclosed under stringent conditions (cf. Article 5 Directive 2002/58/EC).

Recital 15 Directive 2002/58/EC says, "traffic data may, inter alia, consist of [...] duration, time or volume of a communication, [...], the beginning, end or duration of a connection."

Internet service providers assign static and dynamic IP addresses. While a static IP address is assigned to one single user, a dynamic IP address is assigned to several users at different times. Therefore, the only possibility to detect the identity of a person using a dynamic IP address is to review the log files of an internet service provider. The log files contain the specific beginning and end of a connection. Only that information, together with a dynamic IP number, reveals a specific subscriber.

In July 2005, the Austrian Supreme Court issued a Decision saying that the name and address of a user is not subject to the communication secrecy as this information does not constitute traffic data and has, therefore, to be disclosed. Presently, this decision is heavily disputed in Austria.

Belgium

A. Implementation of Directives 95/46/EEC and 2002/58/EEC and other legislative developments

Directive 95/46/EEC

No development to report.

Directive 2002/58/EEC

The Eighth Annual Report indicated that the Commission on Privacy Protection (CPVP) had been consulted regarding the bill implementing Directive 2002/58/EEC. Its principal criticisms were included in the Notice of 14 June 2004, page 21. The Act relative to electronic communications, which introduced the Directive on Privacy and Electronic Communications of 12 July 2002 into Belgian law, among other European directives, was finally adopted on 13 June 2005.

This adds, in particular, two exceptions to the prohibition on electronic eavesdropping, on gaining knowledge of the contents of, and on the recording of, electronic communications as guaranteed by Articles 259b and 314b of the Penal Code. Thus, without prejudice to application of the Act of 8 December 1992 on privacy protection with respect to the processing of personal data (Belgian reference framework), the recording of an electronic communication and of the relative traffic data within the context of lawful commercial transactions **as proof of a commercial transaction or of another professional communication** is authorised on the condition that the parties involved in the communication have previously been informed of the recording, why it is being made and how long the recording will be retained. Gaining knowledge of, or recording, electronic communications and data traffic solely for the purposes of **controlling the quality of call-centre service** is also authorised on the condition that the individuals working in call centres have been informed of the possibility of this taking place and why, and of the period of the recording will be retained (which may not exceed one month).

The Eighth Annual Report also pointed out that the draft bill did not incorporate Article 13 of the Directive into Belgian law. The justification put forward for including the Directive in the 11 March 2003 Act on the Information Society had been criticised by the CPVP on the basis that the Act applied to a different field to the Directive. The CPVP also pointed out that this inclusion did not cover fax machines and other automated calling machines. These objections were partially accepted since the Act of 24 August 2005, which included certain provisions of the Distance Financial Services Directive and of the Privacy and Electronic Communications Directive, did incorporate Article 13 and Article 29b had been included in the Act of 14 July 1991 on trade practices, information and consumer protection. Under this Act, the use of automated calling systems without human intervention and of fax machines for the purposes of customised advertising is prohibited unless the recipient of the messages has given previous, specific and informed consent. When any form of publicity whatsoever is sent by means of this communication technique, the sender is obliged to provide clear and comprehensible information regarding the right to object to receiving such advertising in the future. Concealment of the identity of the vendor in whose name the communication is named is also prohibited. Finally, the sender of the message bears responsibility

for proving the legitimacy of the advertising sent by such means. Anyone has the right to notify a specific sender, at no cost and without explanation, of his/her wish to no longer receive advertising sent by means of such techniques. This inclusion of Article 13 remains incomplete given that only "advertising" electronic mail is covered by the Act of 14 July 1991, rather than "commercial" electronic mail, and thus political or charity-related electronic mail is excluded.

Other legislative developments

Electronic administration – automation of the judicial system

The objective of the Act of 10 August 2005, establishing the Phoenix System, as well as draft legislation relative to the electronic procedure being debated by Parliament, is the uniform automation of the judicial system in Belgium. The Act defines six purposes for data processing by means of this information system: (a) internal communication (management of courts and tribunals and of case files of proceedings) and external communication (notification, serving, communication of judicial acts) required for the functioning of the justice system; (b) management and storage of judicial data; (c) the establishment of a national roll; (d) the setting up of a jurisprudence database; (e) the processing of statistics, and (f) support for justice management and administration.

In addition, the Act provides for a management committee, a supervisory committee and a user committee for the information system. The supervisory committee, a sectoral committee set up within the CPVP, expresses Opinions on its own initiative or on request concerning any question relative to the application of the Act of 8 December 1992 concerning the protection of personal data. It also handles complaints relative to the application of this Act within the framework of the Phoenix System and, within this context, fulfils its mission of mediation and of providing information to the public prosecutor's office regarding any infractions that come to its attention.

Electronic administration – the e-health project

In the area of health, the Government is developing both telemedicine applications and a project involving the processing and automation of data. This project raises numerous questions in relation to (a) the definition of personal, health-related data; (b) the introduction of a personal health-identification number enabling each citizen/patient to access all of his/her health records by means of encoded data, and (c) institution interconnection., In addition, there are question in relation to the objectives of the setting up of such databases and their access procedures as well as their close connection to the social-security system.

B. Jurisprudence

There are no significant developments in this area apart from the Court of Cassation judgment of 2 March 2005, which has already been commented on in the Eighth Annual report relative to 2004 (page 21 and subsequent pages).

C. Various important questions

General

Overall, 2005 saw a continuation of the recent trend towards decentralisation and interconnection of personal-data files. This trend

is part of a context in which security, in the sense of both public security and financial/commercial security, is of growing importance. In its Opinions expressed and positions adopted in 2005, the CPVP often focused on the necessary respect for the principle of file compatibility, in order to avoid systemic crossing of data, and on the transparency for citizens of such processing.

Police and security sectors

The public-authority projects on which the CPVP expressed an Opinion include the project to set up a federal body (OCAM – Coordinating Body for Threat Analysis) with the task of assessing terrorist and extremist threats likely to jeopardise the security of the State or of Belgian interests. The collection of information by this body depends not only on police participation but also on points of contact in various federal public services. The CPVP insisted on the necessity, a fortiori, given that this information is pooled from various sources, of specifically determining the project's objectives, on the importance of rigorous assessment of the pertinence of the data provided and on harmonisation of guarantees protecting data destined to circulate, within a police context, beyond the borders of the European Union.

Identifiers

Within the perspective of limiting the risks of data crossing and coupling, the CPVP also drew attention to certain principles regarding the significance of individual identifiers. In the health sector, it argued that data processed as part of the Cancer Register should be identified by means of a specific sectoral identifier and not by means of a national-register number.

The CPVP expressed major reservations regarding the inclusion on the electronic identity card of certain data, such as that on choices made regarding organ donation and regarding the use of the identity card as an access key to personal medical files. In particular, the CPVP pointed out that the inclusion on the electronic identity card of data extraneous to the identification and authentication of the individual concerned would constitute a dangerous precedent.

Attention was also drawn to a certain degree of confusion in the banking sector which is authorised to use data on the identity card only for the purposes of combating money laundering and not for specific purposes such as customer management. More generally, the collection of data by financial institutions as a prerequisite of national and international rules concerning the fight against money laundering and terrorism raises a certain number of questions that the CPVP is examining in consultation with the Banking and Finance Commission.

Blacklists

At the request of the Government, the CPVP developed principles intended to provide a legal framework for blacklists. Risk management and the necessity of taking positive action against all defaulting parties has led to an increase in such lists (see also the working paper produced by Working Party 29 – WP 25 – of 3 October 2003 regarding blacklists). The CPVP points out that the setting up of such lists could jeopardise a fundamental right (list of defaulting renters – the right to housing; list of dangerous patients – access to healthcare). It describes the defining elements and refers to guarantees for the processing of these lists. The CPVP is

of the opinion that, among other guarantees, the collection of sensitive data (health-related or legal data, data relative to ethnic origin, religion, etc.) should be subject to specific legal authorisation.

Privacy protection in the professional context

The CPVP also expressed its opinion on various aspects of privacy in the professional context in respect both to data on employees and to that on administrators/managers. It also expressed an opinion on various draft bills that, in the name of good corporate governance, provide for the publication of financial data relative to various individuals holding positions of responsibility within companies listed on the stock exchange, public enterprises and publicly subsidised organisations and associations. Without questioning the principle of targeted publication, the CPVP, based its Opinion primarily on the jurisprudence of the European Community Court of Justice, and drew attention to the necessity for balance (proportionality) between legitimate monitoring, on the one hand, and the protection of the privacy of the individuals concerned on the other.

The CPVP also issued an Opinion on the use of badges and on employee tracking by means of a GPS tracking system. Applying the principle of proportionality, which is of particular significance in the implementation of this type of processing, the CPVP pointed out that continual surveillance of employees was to be considered as disproportionate and unnecessary. The CPVP also developed this point of view with respect to the use of biometric data in the context of badge systems used to monitor the hours of an employee's presence at the workplace. In the case of both geographic tracking and of the collection of biometric identifiers, the particularly intrusive nature of this type of surveillance must be proportionate to the objective pursued.

Finally, still within the professional context, the CPVP received numerous questions and requests for information, along with one complaint, in relation to the introduction of professional, ethical guidelines within enterprises concerning whistle-blowing. (See also Opinion 1/2006 of the Working Party – WP 117 – of 1 February 2006 in relation to the application of European data-protection rules to internal whistle-blowing mechanisms in the areas of banking, accounting, internal accounts-control, auditing, the fight against corruption and financial infractions.)

Marketing

Marketing practices were also closely examined by the CPVP, both through active follow-up of complaints from individuals and through co-operation with national and international authorities. Most of the complaints concerned the difficulties that individuals encounter in exercising their right to object to processing of their data for marketing purposes.

Cyprus

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Within the framework of the Structured Dialogue between the European Commission and the Cyprus DPA Office, it was pointed out that some provisions of the Processing of Personal Data (Protection of Individuals) Law of 2001 of the Republic of Cyprus were not fully in line with the provisions of Directive 95/46/EC. These provisions primarily concerned the transfer of data to third countries, the right of information and other procedural issues. The Office has taken into account these points and is in the process of preparing an amendment of the Law.

The Office submitted a proposal to the Office of the Commissioner for Electronic Communications and Postal Services Regulation for the amendment of Part 14 of The Regulation of Electronic Communications and Postal Services Law of 2004, which included the provisions of Directive 2002/58/EC. Among the proposed amendments was the inclusion of the provisions of Article 16 of Directive 2002/58/EC (transitional arrangements) into this Law.

The Office also proposed that the amending Law included references to the Orders on Legal Entities for Unsolicited Communications and Data in Public Directories issued by the Commissioner for Electronic Communications and Postal Services Regulation in 2005 in the section of the Law that deals with telephone directories.

The Road Traffic Offences (Use of Automatic Detection Devices and Other Relevant Matters) Law of 2001 was put into effect in 2005. The Law provides for the recording of certain traffic offences. Under the provisions of this Law, the Council of Ministers appointed the Deputy Chief of Police as the person responsible for the operation and use of these devices.

The Law for safeguarding and protecting the rights of patients was put into effect in 2005. The Law provides among other things for the obligations of persons who provide health services regarding the processing of medical data and the rights of patients regarding the processing of their personal data.

B. Major case law

In the course of examining a complaint submitted to the Office that involved unsolicited advertising SMS messages (short message service – text messages), an audit of the data controller's company that sent the SMS was performed. The audit showed that the company's action was in breach of the provisions of The Regulation of Electronic Communications and Postal Services Law of 2004 and the Commissioner issued a Decision by which a fine of CYP1 500 was imposed on the company.

A couple complained to the Office that their wedding photographer used, without their consent, their photos in an advertising flyer he published. When the photographer failed to comply with the Office's instructions to withdraw the photos, the Commissioner issued a Decision by which the fine of CYP1 000 was imposed on him.

The Office received a number of complaints which involved the practice of several government departments of not informing applicants of the results of written or oral

examinations they took for purposes of employment in the public service. The Commissioner's Office addressed a Circular to all government departments instructing them to comply with the relevant provisions of the Law regarding the applicants' right of access.

C. Major specific issues

Awareness

In association with the Technical Assistance Information Exchange Unit (TAIEX), the Cyprus DPA Office organised a Seminar in Nicosia on monitoring at work, which was aimed at employers and employees both in the public and private sector. The Seminar focused on the legal basis for monitoring, the rights of employees and the obligations of employers under the provisions of the Data Protection Law.

The European Data Protection Supervisor, Mr Peter Hustinx, was invited to deliver a speech on the Lawful Processing of Personal Data at an event organised by the Office in Limassol. The speech addressed members of the Judiciary and the Advocates Associations of Limassol and Paphos.

The Commissioner issued Guidelines on the Processing of Personal Data in the Employment Sector. The Guidelines were published in a booklet form, which, as a first step, was distributed to employers and employees through the Cyprus Chamber of Commerce, the Federation of Employers and Industrialists and several major Trade Unions.

Following the Commissioner's suggestion, the Cyprus Academy of Public Administration and the Cyprus Police Academy have introduced the topic of personal data protection into some of their courses. The Commissioner's staff has been invited by the Academies to give lectures to civil servants and members of the Police on the obligations of Civil Service and Police with regard to the processing of personal data.

Audits and field inquiries

The Commissioner's staff conducted an audit to evaluate Police compliance with its obligations regarding the processing of data in the Police's central automated database, the Schengen Information System (SIS) database (which is under construction) and the Eurodac database. The audit established that overall the Police's level of compliance was satisfactory, but the Office made several recommendations and suggestions in order to ensure that the processing was fully in line with the provisions of the Law.

The Notifications, which an airline company submitted to the Office, did not adequately describe the company's filing systems. In the correspondence that followed, a number of questions arose. The Commissioner's staff visited the company's offices to acquire information in order to verify that the processing of data described in the submitted Notifications corresponded to the way the company actually processed data in these filing systems.

The Office received a number of complaints regarding unsolicited SMS messages that a company sent without the prior consent of the recipients. An audit at the company's office was conducted and it was prima facie established that the company's action was in breach of the Law. A formal decision will be issued after the company presents its case.

Opinions and Guidelines

The Commissioner issued a number of Opinions and Guidelines regarding the lawful processing of personal data, both in the private sector but mainly in the public sector.

In three Opinions regarding the data processed by controllers in the public sector, the Commissioner recommended the amendment of the relevant Law or Regulations so that the processing of data is in line with the provisions of the national data protection Law. These Opinions referred to:

(a) the deletion of excessive information collected through the application forms for employment in the public sector,

(b) the amendment of certain Laws, which provided that for the purpose of issuing certain licenses, the competent authority requests the Police to verify the "good character" of the applicants and,

(c) the amendment of a Regulation which provided for companies that hire vehicles to communicate every day to the Police data centre relating to the identity of all the persons who hired vehicles.

In the first two cases, the data controllers responded positively to the Commissioners' recommendations, whereas, in the third case, a definite answer has not yet been received.

In an Opinion regarding the obligation of government departments to communicate personal data to the House of Representatives in the course of its exercise of Parliamentary Control, the Commissioner recommended that the Departments provide the required personal data to the House of Representatives, provided that this data is relevant to the subject under consideration.

Notifications

During 2005, a total of 108 notifications were submitted to the Commissioner's Office, mostly by controllers in the private sector. It is believed, however, that there are still a number of controllers who have not yet fulfilled their obligations regarding the submission of Notifications.

Complaints

153 written complaints were submitted to the Office during 2005. In addition, numerous complaints by telephone were received and which mostly involved spam and unsolicited SMS messages.

A smaller number of complaints involved the exercise of the right of access.

Licenses

During 2005, the Commissioner received 16 applications for a license to transfer data to third countries. In two cases, a license was granted while in three other cases licenses have been refused. The remaining cases are still pending.

The Commissioner also received 9 applications for combination of filing systems and issued five licenses allowing such combinations.

Czech Republic

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The basic legal regulation for personal data protection is Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Related Acts (hereinafter referred to as 'Act 101'), which came into force on 1 June 2000. This Act established the Office for Personal Data Protection with all necessary powers including the direct imposition of financial penalties. The Act also implemented the Directive 95/46/EC into the Czech legal code. With effect from 26 July 2004, Act 101 was amended by Act No. 439/2004 Coll., which brought it into accordance with the aforementioned Directive.

In 2004, the year of accession of the Czech Republic to EU, implementing Directive 2002/58/EC was succeeded only partly. Act No. 480/2004 Coll., on certain information society services, which came into force on 7 September 2004, includes particular provisions on unsolicited communications. This Act gave the Office for Personal Data Protection new strong competence in the fight against unsolicited commercial communications, including the power of imposing heavy punishment, in those cases of a breach of the law. Directive 2002/58/EC was essentially implemented afterwards by the Electronic Communications Act No. 127/2005 Coll. which went into effect on 1 May 2005. This Act simultaneously implements quite a number of another Directives belonging to the so-called "telecommunication packet". The difficult legislative process of incorporating Directive 2002/58/EC into national law brought about some minor imperfections in Article 7 of Act No. 480/2004 which was criticised by European commission. These imperfections will be set right by expeditious amendment in the first half of 2006.

In accordance with the Legislative rules of the Czech Republic's Government, the Office is the mandatory point to which drafts of relevant Acts are submitted along with other regulations for observation within the framework of interministerial proceedings, thus even before submission of the draft to Parliament. In 2005, the Office expressed its Opinions on a number of legal regulations. Among the significant cases can be mentioned suggestions to the draft of the Act amending some Acts in the area of travel documents, which fulfil EU regulations imposing implementation of biometric data into travel documents. The aim of the Office was primarily to prevent the extension of the scope of scanned fingerprints over the necessary framework required by Council regulation 2252/2004 and the further aim was to safeguard for data subjects the correctness of data verification when issuing of travel documents.

B. Major case law

Decisions made by the Office in two cases were challenged by an administrative action during 2005: a ruling has not yet been made on these actions. Two cases from 2004, as well as one case from 2002, are still pending. The above-mentioned oldest unresolved case is concerned with a financial institution that was not able to effectively protect the personal data of its clients and whose electronic equipment containing records of personal data of several hundreds of thousands of clients was stolen. The Decision of the Office to impose a fine was contested by an action of 2003, which was rejected by the Municipal Court in Prague in 2004, thus upholding

the Decision of the Office. The financial institution then challenged the decision by a complaint which, however, has not been decided on by the Supreme Administrative Court to date.

Another case which is still pending before the courts is a Decision of the Office through which it refused to grant a natural person the status of a participant in administrative proceedings held in 2004. The affected person lodged an administrative action against this decision, which was rejected by the Municipal Court in early 2005, whereby, as in the previous case, it upheld the Decision of the Office. This Decision was also contested by a complaint, which has not been decided on by the Supreme Administrative Court to date.

The other 2004 case is also concerned with a Decision of the Office to impose a fine for unauthorised personal data processing in connection with resolutions of the municipal authorities of a city that were published in full wording (i.e. without respecting personal data protection) on the website of the municipal office. In October 2004, the Decision of the Office was challenged by an administrative action, which has not been dealt with by the Municipal Court in Prague to date.

C. Major specific issues

Control activities performed by the Office in 2005 included mainly ad hoc controls, i.e. examination of complaints. A total of 80 ad hoc controls were carried out, of which 68 were completed. A total of 133 complaints were thus resolved. Certain complaints were handled by inspectors in a manner other than through control, i.e. by remedying the state of affairs. Controls were carried out in banks and leasing companies, business and construction firms, health-care facilities and pharmaceutical companies, and also in governmental agencies and self-governing bodies. Several comprehensive controls were also performed on the basis of the control plan:

Cases of violation of the law ascertained in 2005 were concerned especially with:

- unauthorised processing of inaccurate or excessive data
- unauthorised transfer of data to another controller
- insufficient or incorrect information on the data subjects
- processing of sensitive data without express consent of the data subject
- poor securing of personal data, e.g. as a consequence of unsuitable access rules in an information system allowing access to personal data by unauthorised entities.

Instigations and complaints received by the Office during the previous year particularly concerned the following areas:

1) Public registers. A majority of instigations and complaints were aimed against the excessive extent of publication or provision of personal data and copies of instruments containing such data. This is true, e.g., the Commercial Register is still the subject of discussions related to the justification of publication of a certain group of personal data, including the birth dates, in relation to the purpose for which the Commercial Register was established.

2) Publication of data from meetings of municipal boards and councils, particularly on the Internet. The number of complaints in this area has decreased compared to 2004 after an updated Opinion and Guideline was issued by the Office, as the competent institutions adopted the desirable measures and the relevant personal data contained in municipal documents became accessible as stipulated by special laws providing for competence of the municipal bodies.

3) Processing of personal data in the area of municipal services. It can be stated on the basis of complaints received by the Office that, in this area, citizens are not always adequately advised of activities performed by private entities authorised by public self-governing bodies. It shows that the provision of services by public institutions to citizens necessarily entails provision of information with respect to the rights and obligations of the citizens; the right to process data must be firmly connected to the duty to advise the data subject of personal data processing.

4) Management of personal data of employees. Instigations often indicate that management of personal data could serve, *inter alia*, as a means of exerting pressure in the resolution of labour-law disputes. Such instigations are discussed in co-operation both with Labour Offices and, where appropriate, with the newly established Labour Inspectorates (from 1 July 2005).

5) Copying of personal documents. Amendments to the Acts on Identity Cards and on Passports (effective from 1 January 2005) proved unambiguously beneficial in this respect; infractions consisting in copying of documents without the citizen's consent are now punished by municipal authorities. However, the Office continues to act in cases where a copy of the personal document is required particularly for conclusion of a contractual relationship and it also assesses the necessity and manners of use of all personal data set forth on a copy of a document, where it particularly points out that unnecessary collection of personal data could be taking place.

On the basis of control findings of the Office's Inspectors, a number of financial penalties were imposed, for example:

In connection with the performance of powers of the Office pursuant to the Personal Data Protection Act, the heaviest fine in the previous year was imposed on a civic association which, in an attempt to bring attention to the subject of regulated rents, sought out, associated and then published on its website personal data of specific tenants of apartments who, in its opinion, did not require relief provided by means of regulated rent. Identification data of the affected data subjects, including the birth date, and sensitive personal data indicating their political preferences were processed in this manner, together with information on their real estate including lists of ownership titles and extracts from the Land Registry.

The Office also imposed a heavy fine on a housing co-operative which, in connection with the exercise of rights and obligations in administration of an apartment building, installed and operated a camera monitoring system in the building, by means of which personal data of tenants of apartments in the given building were processed without their consent. The installed cameras were operated continually and they recorded common premises of the building

in such a manner that every person who entered or left his or her apartment had to pass through such premises; the resolution of the cameras was sufficient to identify persons and their activities. Electronic locks were also installed in the building, where each of the residents had a specific identifiable chip to such locks. Premises where electronic locks were installed were also covered by cameras. Recordings from the cameras and recordings from the electronic locks constituted a comprehensive information system, with the use of which it was possible to obtain information on movement and activities of natural persons, i.e. tenants, members of the co-operative and other visitors, on the common premises of the building.

Another fine was imposed on a state body in relation to scanning of biometric data and pictures of fingerprints. Data on fingerprints were routinely acquired at variance with the special laws regulating the procedure of the body also with respect to persons who did not meet the requirements for permitted taking of fingerprints, as specified by the special laws, and, moreover, data on fingerprints were not processed separately within the performance of various tasks of the body.

The Office also imposed heavy fines within the performance of its new competence pursuant to the Certain Information Society Services Act. This competence covers the area of sending unsolicited commercial communications, alias commercial spam.

Denmark

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The Act on Processing of Personal Data (Act No. 429 of 31 May 2000) was adopted on 31 May 2000 and entered into force on 1 July 2000. The English version of the law can be found on the following address: http://www.datatilsynet.dk/eng/index.html

The Act implements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2002/58/EC was incorporated into national law in Denmark by:

- The Danish Constitution
- Law on Marketing Practices, Section 6 (cf. Law no. 1389 of 21 December 2005)
- Law No. 429 of 31 May 2000 on Processing of Personal Data
- Law on Competitive Conditions and Consumer Interests in the Telecommunications Market (cf. Exec. Order No. 784 of 28 July 2005)
- Executive Order No. 638 of 20 June 2005 on the Provision of Electronic Communications Network and Services
- Chap. 71 of Law on Administration of Justice, cf. Exec. Order No. 777 of 16 September 2002
- Section 263 of the Penal Code, cf. Exec. Order No. 779 of 16 September 2002

According to section 57 of the Act on Processing of Personal Data, the Opinion of the Danish Data Protection Agency (DPA) shall be obtained when orders, circulars or similar general regulations of importance for the protection of privacy in connection with the processing of data are to be drawn up. The provision also concerns bills. The DPA has given its Opinion on several laws and regulations with impact on privacy and data protection.

1. In 2005, like in 2004, the DPA has focused a great deal on the upcoming reform of the structure of the public sector.

The DPA was asked to comment on an order regarding the processing of personal data by the municipal citizen service on behalf of the National Tax Authorities in tax matters. The arrangement would mean that municipal authorities gained access to all the data in the tax authorities' system.

The DPA noted that transfer of data to a processor must be based on a written agreement between the parties. It was the opinion of the DPA that such an access would actualise the need for additional safeguards to be implemented, and that access to data should be given according to geographic and organisational status.

2. The DPA was asked to comment on a bill introducing an electronic income register containing information regarding monthly income and employment status. The purpose of the register was to simplify the communication between citizens and companies by making sure that no one should have to provide the same information twice.

The DPA noted that, besides from a more efficient communication, the register also facilitated control of citizens, and found that it should be specified in the act, to which extent authorities could check on citizens using the register.

The DPA noted that access to the register demanded that this be specifically mentioned in other legislation and underlined the importance

of assessing in each case whether access to the register is necessary.

3. A new Danish legislation on internet domains was adopted in July 2005. According to the new law only registrants can become anonymous in the Whois register and it requires that the person is registered for anonymity in the Danish citizen register (CPR) and/or in the telephone register. The DPA remarked that in principle all citizens should have the opportunity to be anonymous in public registers.

B. Major case law

1. Following the notification of processing of personal data about juvenile sexual offenders, their families and victims, the DPA stated that offenders and their families must consent to the processing. Regarding processing of data about victims, the DPA stated that it may not always be possible to obtain consent from the victim, and that information can be processed without consent if it is *necessary* to give the juvenile offender the best possible treatment.

Based on lack of notification and adequate safeguards, the DPA notified the relevant Ministry that the Act on Processing of Personal Data had not been abided by.

2. The Danish libraries asked the DPA to inform them whether it would be in accordance with the data protection Act to send information on the reservation of library books to citizens by e-mail without encryption.

The DPA was of the opinion that data regarding a person's choice of library books is confidential and should not be transmitted over the internet without being encrypted. However, due to the small number of citizens able to receive encrypted e-mails, the DPA exceptionally accepted that libraries could, for a five-year period, continue to send these e-mail without encryption. The DPA requested that the libraries use the five-year period to implement systems that heighten the level of security when transmitting information over the internet.

3. The DPA was asked to interpret the rules regarding the right of information in situations where the data subject is a minor.

The DPA was of the opinion that minors should be given information according to the same rules as all other data subjects if they are over the age of 15. Information should in these cases also be given to the child's parent or guardian, unless the information is of such a personal nature that it could be considered a violation of privacy. If the child is under the age of 15, information should be given to a parent or guardian.

C. Major specific issues

In 2005, the Minister of Justice decided to form an expert group to evaluate the existing legislation on CCTV-surveillance, and to gather a basis on which to decide where to draw the line between the need for security and crime prevention, and a citizen's right to privacy.

Among other things, the decision was based on a recent Opinion by the Data Protection Agency, pointing out a series of questionable factors relating to the joint enforcement of the Act on CCTV-surveillance and the Act on Processing of Personal Data.

The expert group will finish the evaluation before 1 September 2006.

Estonia

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

No major developments to report, although the working group is actively dealing with the amendments of Estonian Data Protection Act.

B. Major case law

Citizens versus Estonian Data Protection Inspectorate

Two citizens submitted complaints to the Estonian Data Protection Inspectorate (EDPI) about the Border Guard Administration (BGA) and Public Prosecuter's Office (PPO) for not registering the processing of sensitive personal data with the EDPI. The Inspectorate instituted a misdemeanour procedure concerning the registration, but the EDPI did not accept the applicants' claim to stop the processing of sensitive personal data in the BGA and the PPO and to cancel the sensitive data associated with applicants. In this case the EDPI is of the opinion that the data subject's right to demand the cancellation of his/her personal data and to stop the processing of sensitive data in the authority, is not unlimited. First of all, the authorities have the legal obligation to process this data. And the fact, that the authorities have not registered the processing of sensitive data, is secondary and it should not be the reason to stop the functioning of these authorities.

Applicants were not satisfied with the Decision of the EDPI and they sought redress in the Administrative Court. The Court did not uphold the applicants' complaint and the Decision of the EDPI was sustained.

As a next step the applicants filed an appeal with the Circuit Court, where the appeal was also not upheld.

C. Major specific issues

Through the years the major issue has been problems concerning the processing of data for scientific and statistical purposes.

The latest version of Personal Data Protection Act came into force in October 2003. According to the Act, the consent of the data subject is required for the data processing for statistical, historical and scientific purposes. It is also necessary to register the sensitive data processing with the EDPI to meet the requirements of the Act.

The disagreements with scientists and statisticians are related to the Act and attempts to find solutions are still going on (amendments of the laws, co-operation between the EDPI and the statistical/scientific authorities etc).

Finland

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The Directive of the European Parliament, and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999. The Act was revised on 1 December 2000, when provisions on the Commission's decision-making, as well as how binding these decisions are in matters concerning the transfer of personal data to countries outside the Union under the Data Protection Directive, were incorporated into it.

Protection of privacy has been a basic right in Finland since 1 August 1995. Under the Finnish Constitution, protection of personal data is regulated by a separate act.

The Act on Data Protection in Electronic Communications (516/2004), which entered into force on 1 September 2004, implemented the Directive on Privacy and Electronic Communications (2002/58/EC). The purpose of the law is to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications and the balanced development of a wide range of electronic communications services.

The responsibility for enforcing the law was divided so that the mandate of the Office of the Data Protection Ombudsman includes:

- regulations on processing location data
- direct marketing regulations
- regulations on cataloguing services
- regulations on users' specific right to obtain information.

In this connection, it should be noted that according to the Penal Code, the prosecutor is obliged to consult the Data Protection Ombudsman before pressing charges in a matter concerning a violation of the secrecy of electronic communication.

B. Major case law

In Finland, the amount of domestic junk mail is relatively well controlled when compared to the international situation. It is estimated that the amount of junk mail from Finnish operators has decreased significantly. However, in 2005 the interpretation of Section 26 of the Act on Data Protection in Electronic Communications became a major problem. According to the section, a seller who has received a customer's electronic address in conjunction with a sales transaction can use that address to send marketing messages appertaining to the seller's own identical or similar products or services without prior consent from the data subject, which is otherwise the rule. The problem was how to define "similar". In most cases it seemed that the data subjects who had lodged complaints did not even know that they had a customer relationship with the company sending the marketing messages, even though the Personal Data Act includes the duty to inform them on the processing of data.

As regards telephone directory and number services, the Office of the Data Protection Ombudsman produced a report in summer 2005, which revealed that operators did not

inform the subscribers sufficiently widely and accurately about their rights and the directory services where subscribers' information was entered. On the other hand, according to the report the operators seemed to give adequate information to the data subjects about the use of localisation data.

Currently there are several laws in preparation in Finland that include important regulations on processing personal data. Such laws include the new credit information legislation, population information legislation and the law on the electronic processing of customer data in social and health-care services.

The proposed credit information law would be a comprehensive law encompassing all credit information activities and credit information processing. It would apply to the processing of credit information related to consumers, companies and the people in charge of these matters in companies. The law would regulate the credit information register and the data entered there, as well as on the length of time that the data is kept in the register. The data quality of credit information registers would be improved, for instance, by grading the time the disruption in payments is kept in the register according to whether the data subject has new disruptions in payments, and by also entering background information on disruptions in payments, such as it being related to guarantee liability. The new law would replace the regulations on personal credit information now contained in the Personal Data Act. Control and enforcement of the new law would be entrusted to the Data Protection Ombudsman.

The bill on the electronic processing of customer data in social and health-care services would apply to both internal electronic data processing by the controllers and electronic data transfer between different controllers.

The aim of the amendment to the Population Register Act is to achieve legislation that better and more accurately directs the maintenance, utilisation and systems, and service development of the data contained in the population information system and certified electronic transactions. The reformed legislation aims at better taking into account the citizens' fundamental rights, especially the protection of privacy and personal data, and legal protection and good governance.

C. Major specific issues

The number of cases processed by the Office of the Data Protection Ombudsman increased by approximately 20% from 2004 to 2005. In 1998, the proportion of complaints directed at the private versus the public sector was 1:1.17, whereas, in 2005, the proportion was 1:1.74. That is, every complaint directed at the public sector was matched by nearly two complaints directed at the private sector.

The reason for this development is probably that personal data processing by public authorities is usually regulated by law, in accordance with Section 10 of the Finnish Constitution. In addition, the public sector has central national-level control. It is organised under development programmes at national and local government levels. The figures, however, show that the change in the proportion is not so much due to improvement in the public sector, but deterioration in the private sector. Indeed, private companies try to test the boundaries of the law.

A representative from the Office has attended approximately 30 different working groups or similar bodies appointed by various authorities. Especially important has been co-operation with the Steering Committee for Data Security in State Administration (VAHTI). In addition, there has been regular informal co-operation with numerous other interest groups. Last year, 2005, saw the issuing of 45 statements on legislative matters and 20 on administrative reform projects. A representative of the Office was heard at the Parliament 29 times during the year.

The role of data and data processing in society has changed in the information society as data processing is beginning to be understood as part of the implementation of each basic process. Data protection and security are now being integrated into processes. Simultaneously, there is increasing awareness of the fact that data is capital that needs to be protected and managed. Data processing also needs to be directed. Data security is beginning to be understood as a range of means for taking care of the judicial quality of services and other processes. Fortunately, data security is no longer seen as an exclusively technical activity. Instead, it is understood that direction, training and planning are also means of implementing data security.

The importance of data protection and the significance of promoting it have become increasingly clear as a means to strengthen people's confidence. There is growing awareness of the fact that each data system solution is also a measure to safeguard the citizens' fundamental rights. The implementation of new technologies increasingly takes into account the data protection and security risks that they pose not only to the citizens, but also to the entire system.

Reconciling data protection and problems caused by the Internet has succeeded fairly well. Identity theft has not so far become a particularly common problem in Finland, unlike in some other countries. However, increased online transactions using the Internet and mobile services have indicated that this problem also exists in Finland. Because of this, the Office of the Data Protection Ombudsman published several Guidelines on this and related topics.

As regards public administration, the Ministry of the Interior commissioned a report at the end of 2005 on public online services. The report showed that people are now more cautious about using their bank or credit card information or personal data on the Internet. People's data security skills were improved by, for instance, organising a national data security campaign and day, which even attracted attention abroad. At the end of 2005, the Information Society Council also organised a campaign aiming at increasing public awareness. The materials and themes of both campaigns had sections and guidelines related to the processing of personal data.

Information dissemination over the Internet by municipalities and the related processing of personal data have raised many questions from the citizens. It is therefore important that the Association of Finnish Local and Regional Authorities in 2005 published new guidelines for information dissemination over the Internet.

The Ministry of Transport and Communications began a two-year programme called LUOTI in 2005. The programme aims at discovering what data security challenges the development of electronic services in the near future, how to prepare for them, what solutions there are and how they should be developed. The programme's

participants include representatives of the public and private sectors alike. The fundamental objective of the programme is to increase consumer confidence in the new electronic services. A central means for gaining that confidence is learning to take care of data protection and security.

France

A. Implementation of Directives 95/46/EEC and 2002/58/EEC and other legislative developments

The Act of 6 January 1978, amended, and its implementing order of 20 October 2005

The European Directive of 24 October 1995 was incorporated into French law by the Act of 6 August 2004 which amended the Act of 6 January 1978. The implementing order of the new Act on Informatics and Freedoms was adopted on the 20 October 2005. These texts contained major changes.

1. The "Informatics and Freedoms Officer"
As a result of the Act of 6 October 2004, enterprises, local governments, public institutions and associations must appoint an informatics and freedoms officer. However, these bodies are exempted from making declarations to the CNIL (National Informatics and Freedoms Commission). This major innovation constitutes a turning point in application of the Act: the focus has been placed on education and advice upstream. The appointment of an officer certainly makes it possible for those responsible for data processing to benefit from a relaxation of declaration obligations. In particular, it makes it possible for them to comply better with their legal obligations in relation to security, transparency, and proportionality as to the processing of data and to the rights of individuals. Heavy sanctions are applied in the case of default. The appointment of such officers makes available to those responsible for data processing a specialised expert able to provide them with advice, to make recommendations, to provide training and to alert them to cases of serious malfunctioning. As of 31 December 2005, 73 bodies had designated such officers.

2. Simplification procedures
The simplification of preliminary procedures is one of the principal themes of the new Act. In compliance with the legislators' intention and with its European commitments, the CNIL began to make use of all of the simplification instruments provided by the new Act (declaration exemptions, adoption of new and simplified rules, individual authorisation decisions, advice on individual regulatory acts, etc.). This process of simplification of preliminary procedures remains a focus for the CNIL in 2006.

3. Validation of codes of conduct
The amended Act of 1978 authorises the CNIL to express an Opinion on the conformity of the provisions of French law and data-protection regulations regarding "professional rules for protection of personal data". In 2006, the CNIL validated two projects concerning "e-mailing codes of conduct" that were negotiated with the industries concerned.

4. Supervisory role
The new Act gave the CNIL wide-ranging supervisory powers. During 2005, it carried out approximately 100 inspections (an increase of 235% over 2004). It is expected that this figure will increase significantly in the years to come. The principal activity sectors monitored were:
- mass distribution
- direct marketing
- biometrics
- video surveillance on private premises
- Internet insurance brokerage.

In addition, an audit of on-line banking services requested by ten banking institutions was carried out during the first half of 2005 based on a type of questionnaire. This enabled CNIL to formulate recommendations, which are available

on its website, for both banking institutions and Internet users.

5. Restraint Board sanctions
The new Act set up a specific board, the Restraint Board, within the CNIL with the task of prescribing sanctions. During its first year of operation, the Board was able to test the new sanction mechanisms at the procedural level and with respect to specific cases files to be examined. In 2005, the Restraint Board met eight times and examined 50 case files.

These case files concerned, for example:
- lack of respect for registration requirements in a Banque de France case
- difficulties encountered in exercising the right to access or objection to receiving commercial prospecting
- the existence of illegal "block note" areas
- the setting up of illegal infraction files
- unauthorised third-party access to data.

The Restraint Board also applies sanctions to procedural defaults: for example, the lack of request for authorisation prior to the setting up of certain files and the lack of response to e-mails requesting additional information during various procedures.

In order to impose a financial sanction, the CNIL is first required formerly to demand that the observed defaulting behaviour cease. The CNIL may only decide to impose financial sanctions in cases in which its formal requests are ignored. In 2005, the 35 notifications sent to respondent bodies had, overall, an extremely salutary effect, with 85% of these bodies complying and regularising their actions. The financial sanction is not the only possible response. The Restraint Board found that orders to cease certain data processing or public announcements were often more appropriate.

6. International data transfers
The Act of 6 August 2004 empowers the CNIL to authorise, in certain cases, international data transfers to countries outside the European Union. It is of great concern to the CNIL that the various conditions to which such international data transfers are subjected should be consistently and effectively defined. It therefore accepted, on 30 June 2005, that the internal rules (BCR – Binding Corporate Rules) of the General Electric Group (GE) could validly be used as a framework for the numerous international data transfers carried out by GE for the purposes of human resource management. More generally, the CNIL worked with its European counterparts in order to advance several similar case files, in order to ensure the legitimacy of internal rules at the European level and to promote such rules among the enterprises concerned. It also submitted a major working paper produced by the Article 29 Working Group, regarding common interpretation of the so-called "exceptions to Article 26-1 of Directive 95/46 EEC of 24 October 1995". It also worked to simplify and make more effective the procedures and formalities applicable to international data transfer at the national level.

Implementation of Directive 2002/58/EEC

European Directive 2002/58/EEC was incorporated into French law by the Act on Confidence in the Digital Economy (LCEN) of 21 June 2004. The LCEN is intended particularly to counteract spam by reinforcing protection for e-mail users. It introduces a rule requiring prior consent (opt-in) to the electronic sending of commercial messages by means of SMS (Short

Message Service) or MMS (Multimedia Messaging Service). The user's agreement must be given in full knowledge of the purpose. In addition, it is the CNIL's view that physical persons may be prospected by e-mail through their professional e-mail addresses without their prior consent if the message is sent to them in the capacities they fulfil within the private or public body that provided them with the addresses used. For non-commercial approaches (political, associative, religious or charity-related prospecting, for example), the general data-protection rules apply: prior information on the use of the e-mail address for such purposes and the right to object, at no cost, to such use (opt-out).

Other Legislative Developments Relative to Data Protection

1. Antiterrorist legislation (Act 2006-64 of 23 January 2006 relative to the fight against terrorism)

In 2005, the Ministry of the Interior officially consulted the CNIL with respect to its draft bill on the fight against terrorism, which provided for personal-data processing in various areas (video surveillance, transmission to the police services of data on passengers travelling to or from the EU, the setting up "at all appropriate points" on the road network of devices to record license plates and to photograph vehicle occupants, access to Internet-connection and telephony data, anti-terrorist service consultation of certain administrative files kept by the Ministry of the Interior, etc.).

In its Opinion of 10 October 2005 the CNIL pointed out that the objectives pursued were legitimate but called for particular guarantees in order to maintain the balance between national-security needs and the protection of freedoms. The CNIL was particularly concerned that the fight against terrorism should not lead to files and video-surveillance recordings being made available to police and gendarmerie services, resulting in a large part of the population being tracked systematically and permanently when moving from place to place and when involved in various aspects of their daily lives. The legislator did not take all of the CNIL's concerns into consideration however and it has also allowed for the limiting of the information communicated to the CNIL when the latter is required to express an Opinion on files of interest to State security, defence or public safety.

Several provisions of the act of 23 January 2006 expand the use of the connection data that communication operators are required to store according to the Act of 15 November 2001 on daily security. The Act extends the definition of an "on-line communication operator" in order to oblige not only "classical" operators to keep such data but also cybercafés, restaurants, hotels, airports, etc., when such enterprises offer access to the Internet. While pointing out that this obligation did not require cybercafés in particular to identify the users of electronic-communications services, the CNIL requested (unsuccessfully) that the categories of individuals concerned be specified so that libraries, town halls, universities, etc., offering Internet connection would be able to determine whether they are, or are not, subject to the obligation to store data. The Act also henceforth allows, without control by the judiciary, individually authorised national police and gendarmerie service agents in charge of the fight against terrorism to access technical data stored by electronic-communications operators.

2. The Act of 12 December 2005 on penal-offence recidivism and the electronic bracelet
The placing of individuals under mobile electronic surveillance is one of the principal provisions of the Act of 12 December 2005 on the handling of penal-offence recidivism. In concrete terms, such surveillance makes it possible to track continuously, by means of GPS or GSM technology, an individual wearing an electronic-monitoring transmitter (tracker). Such surveillance may be used in three distinct legal contexts: social/judicial follow-up, conditional freedom and judicial surveillance. The individual's prior consent is therefore required.

3. The Order of 6 June 2005 and the distribution and reuse of public data
The Order of 6 June 2005 provides for a scheme protecting personal data contained in the numerous documents produced by the public sector (electoral lists, benefit-recipient management files, assessment rolls, tax files, etc.). Henceforth, any reuse of public information containing personal data is subject to the Act of 6 January 1978. As a result, parties providing or requesting such data must declare to the CNIL their intention to reuse that data.

4. The Teleservices Order of 8 December 2005
The Order of 8 December 2005 provided a legal framework for the creation of public on-line services ("teleservices"). It defines the conditions for the paperless exchange of data between administrations and citizens and between administrations. The CNIL has already examined the on-line change of address service, the national portal handling requests for birth-certificate extracts as well as an experimental version of the "monoservicepublic" portal.

5. The consequences of Act 2004-1486 of 30 December 2004 and diversity measurements
The Act of 30 December 2004 led to the setting up of an overall authority for the fight against discrimination and for equality and for the fight against discrimination in the labour sector, particularly discrimination based on ethnic, national or racial origin. It has been the subject of numerous reports and initiatives in recent months.

The tools used to measure diversity are intended to enable employers to gain knowledge of the ethnic and social origins of their employees or potential employees. These tools may involve the collection and processing of data that enable the identification, of the individuals concerned. Now all data on the racial or ethnic origin of an individual is considered sensitive and its collection and use are subject to special precautions.

The CNIL made a number of recommendations in this regard on 5 July 2005. It holds the view that the use of statistical tools to measure diversity in order to fight against employment discrimination is completely legitimate. However, it is of the opinion that there is no reliable basis for comparison currently available in France. In the absence of a national reference of ethno-racial types established on the basis of public statistics, the establishment of such a database must be approved by the legislator. As a consequence, the CNIL recommends that, at this point, employers do not collect data on the real or supposed ethnic origin of their employees or recruitment candidates. It prefers the processing of information on the national origin of individuals such as it already exists in public statistics (nationality, nationality of origin when appropriate, place of birth, nationality

or place of birth of parents) and recommends that the use of this data respects anonymity. It advises employers to enter into a process of prior analysis, in consultation with personnel representatives, in order to clarify the objectives of the diversity policy.

6. The consequences of the American Sarbanes-Oxley Law

On 26 May 2005, the CNIL refused to authorise two whistle-blowing mechanisms. The purpose of these mechanisms was to enable employees and others associated with the companies concerned to inform about supposing wrongdoing attributable to their colleagues. The CNIL based its two decisions on the fact that these particular mechanisms risked leading to "an organised system of professional informing". The impact of these two authorisation refusals was significant both in France and abroad. The enterprises were concerned that, on one hand, they would not be able to comply with personal-data protection rules and with the American Sarbanes-Oxley (SOX) Law on the other. The SOX Law requires the setting in place of whistle-blowing procedures in the financial, accounting and accounts-control fields. The French enterprises subject to this law (either because they were directly quoted in the United States or because they were French subsidiaries of companies quoted in the United States) must certify to the markets concerned that they respect this obligation to set up such whistle-blowing mechanisms on penalty of being delisted. Aware of these difficulties, and not wanting to leave these enterprises in this state of uncertainty, the CNIL took various steps to ensure follow-up to its decisions of 26 May 2005. It therefore adopted, on 8 December 2005, a Decision for individual authorisation of whistle-blowing mechanisms conforming to the guidelines it had established in a framework document on 10 November 2005. In particular, the CNIL recommends that whistle-blowing be limited to certain specific fields (such as accounting, banking, accounts control and the fight against corruption), that anonymous informing should not be encouraged, that a specific organisation be put in place to collect and process such information and to inform the person concerned once proof has been established.

7. The Decree of 27 May 2005 relative to directories and universal information services

The establishment of a universal directory, provided for by the 1996 Telecommunications Regulatory Act, has been subject to numerous delays, particularly due to the evolution of its legal framework. Publication of the Decree of 27 May 2005 definitively completed the legal framework applicable to directories and to universal information services intended to compile the details of all telephony subscribers, irrespective of operator. The communication was sent to the operators' customers at the end of 2005 so that the subscriber lists/user lists could be set up integrating various options relative to personal-data protection. The operators must make these lists available to anyone wishing to produce a universal directory or provide a universal information service, whether at the national or local levels.

B. Major case law

Checking of employees' working hours by means of fingerprints

The High Court of Paris, in a Judgment of 19 April 2005, decided that the checking of employees' working hours by means of fingerprints was

disproportionate. The employer concerned had respected its obligations regarding employees' individual information and prior consultation with employees and had also informed the CNIL of its intentions. Basing its Opinion specifically on the need for proportionality (established in particular by Article L.120-2 of the Labour Code) of the monitoring means put in place relative to the objectives pursued, the Court nevertheless prohibited the company from implementing a biometric-badge system based on fingerprints. The judge thus considered that an employer is not justified in setting up a system of working-hour supervision by means of fingerprints without any proof having been provided that the use of a classic badge would not be just as effective. The Court's Judgment is in line with related decisions taken by the CNIL, according to which all biometric systems for supervising employee access or working hours must be authorised prior to their implementation.

Employer access to employees' hard disks authorised under certain conditions

The Court of Cassation decided, with its Nikon judgment of 2 October 2001, the absolute right of employees in respect to the intimacy of their private lives within the framework of the use of their professional electronic messaging. With its Judgment of 17 May 2005, the Court recognised the right of the employer, under certain conditions, to access the personal files of its employees stored on the hard disks of their computers. The Court did, however, specify that "without risk or prejudice, the employer may not open files identified by the employee as personal and stored on the hard disk on the computer made available to him/her except in his/her presence or that of his/her delegated representative". This Judgment does not affect the application of the principle of proportionality to checks made of employees' "personal" files. In all cases, the employer is obliged specifically to justify any access to files of a personal nature, in compliance with the Labour Code and with relative texts on privacy protection.

A spammer is sentenced

With a Judgment of 18 May 2005, the Paris Court of Appeal imposed a fine of 3 000 on a spammer denounced by the CNIL. This judgment confirmed the CNIL analysis, according to which the collecting of e-mail addresses, without the knowledge of the individuals concerned and in the public domain of the Internet, makes it possible to indirectly or directly identify a physical person and this contravenes legislation on data protection. An appeal has been launched with the Court of Cassation regarding this Judgment.

C. Various important questions

Electronic identity

On 22 November 2005, the CNIL expressed gave an Opinion on the decree instituting the electronic passport and on the procedures for its secure production. Equipped with a contact-less chip, the new passport will integrate the digitised photograph of its holder. Passport photographs were already part of personal data processed in the issuing of passports but the decree provides that, from now on, they must be integrated in a digitised form and stored in a contact-less chip. The CNIL made recommendations to prevent any fraudulent collection of data from the electronic chip and to ensure better control of access to the national passport file.

Concurrently, the INES (Secure National Electronic Identity) project for electronic and biometric identity cards should be operative in 2008. Conceived in compliance with interoperability standards, the electronic identity card will be readable in all countries equipped with contact-less chip card-readers, particularly in Europe. They should also be usable in order to access teleservices by certifying the electronic identity of their holders. The holding of this identity card should remain optional. The data stored in the card's chip will include the holder's digital fingerprints and photograph. The CNIL has been following the development of the INES project for the last few years. This is, in fact, a major societal issue, given that it involves the biometric identification of the entire French population.

Geolocalisation of employee vehicles

The CNIL has received a great many requests for advice and many complaints from employers and employees regarding the legal framework applicable to vehicle geolocalisation. The devices concerned are based principally on use of GSM/GPS technology that, for example, makes it possible to pinpoint a vehicle's position at any given moment. This enables very close supervision of the activity of the employee using the vehicle. Implementation of a geolocalisation tool implies certain risks with respect both to collective rights (the right to unionise, the right to strike) and to individual freedoms (the freedom to come and go anonymously, the right to privacy). Such processing raises two questions: that of the dividing line between work and private life and that of the level of permanent supervision to which an employee may be subjected. The CNIL has already identified the problems relative to use of geolocalisation tools in the professional context. During the first half of 2006, it will adopt a recommendation on the conditions under which such devices may be used.

Parallel judicial records

In 2006, as was the case in 2005, the social consequences of the consultation of police files for administrative purposes remains a major concern for the CNIL which carries out various inspections related to the right of indirect access to police and gendarmerie files. It has observed on numerous occasions that recourse to police files, within the context of administrative inquiries carried out for access to certain security operations or for the swearing in of certain functions, can have dramatic consequences for the individuals concerned. Refusals to hire or decisions to dismiss are in some cases decided solely after consultation of these files and based on sometimes unjustified, erroneous or out-of-date reporting. This administrative use of police files amounts to parallel judicial records without the rigorous guarantees provided by the Code of Penal Procedure for national legal records.

There is the risk that this situation will become more serious. The Decree of 6 September 2005 considerably extends the list of inquiries that may include consultation of police files. In addition, it is to be expected that the areas covered by police working files (STIC) will widen; at the present time, it only involves serious infractions (crimes) or relatively serious infractions (misdemeanours). This extension does not appear in any way justified.

The CNIL does not contest the legitimacy of the objective pursued by the State, which wants to ensure tighter control over so-called sensitive

activities. It does, however, consider it to be prudent to correct the negative effects of a mechanism that was not originally designed for this purpose. The CNIL has submitted to the Government a number of proposals that would remedy this situation.

Stadium violence

The question of stadium security is a very topical one in France, given the increasing number of football events in 2006 and the outbursts that have occurred. Organisers of these events are sometimes legitimately tempted to turn to electronic data in order to select spectators. The attention of the CNIL has been drawn to the conditions according to which the French Football Federation (FFF), on the occasion of the France-Germany match of 12 November 2005, recorded data such as the surnames, names, addresses and identity-card numbers of French spectators. As planned, this operation, which was presented as being in the interests of security, did not respect legal provisions, particularly because the use of this data was not clearly defined and because the CNIL had not been notified of its collection. Subsequent to the CNIL's intervention, the FFF decided to put an end to this operation and to consult with the CNIL in order to ensure that these practices conform to data-protection regulations.

Germany

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

- The Directive 02/58/EC has been implemented partially into German law by revision of the Telecommunication Act in 2004. Its implementation in the field of tele- and media services is still pending.

- Act on the transposition of the Federal Constitutional Court's decision of 3 March 2004 (acoustic surveillance of private homes) of 24 June 2005 (BGBl. I p. 1841)

- Act on the amendment of the forensic DNA analysis of 12 August 2005 (BGBl. I p. 2360).

B. Major case law

In its decision of 18 July 2005 (2 BvR 2236/04), the Federal Constitutional Court ruled that the regulations transposing the Council framework decision on the European arrest warrant and the surrender procedures between Member States (Official journal no. L 190 of 18 July 2002 p. 1) into national law is unconstitutional and, therefore, null and void. Thus, it will not be possible to extradite Germans to another EU Member State until a new law on the European arrest warrant has been adopted. At present, a new draft law is being debated.

In its decision of 27 July 2005, the Federal Constitutional Court ruled that the regulation of the police law of Lower Saxony for preventive monitoring of telecommunications is null and void because it constitutes a violation of the confidentiality of communications which is protected by the Constitution (Art. 10 Basic Law). Among others, the court criticised that the respective legal rules were lacking in definition and clarity. Moreover, the respective regulations do not comply with the principle of proportionality. In the end, the Federal Constitutional Court reaffirmed its opinion stated in past decisions by saying that the inviolable core of privacy guaranteed by human dignity has to be warranted without any restraint if security services carry out covert data collections. In a concrete case, if clues arise substantiating the presumption that in a monitoring measure contents belonging to that core of privacy are included, this measure cannot be justified and has, therefore, to be discontinued. Furthermore, safeguards are required guaranteeing that contents of communications coming from such a highly personal area are not going to be used, but are immediately deleted, if, in an exceptional case, a collection had happened before.

C. Major specific issues

Co-operation of the police forces in Europe

In Prüm, Germany, on 27 May 2005, Belgium, France, Luxemburg, the Netherlands, Austria, Spain and the Federal Republic of Germany signed a treaty on intensifying cross-border co-operation, in particular concerning the fight against terrorism, transnational crime and illegal migration.

This treaty constitutes a milestone in the area of cross-border co-operation in criminal matters and in other fields of tasks. For this purpose, among others, it is envisioned that the contracting parties make their central databases of DNA and fingerprints available to the central contact offices of the other contracting parties via a hit/no hit procedure. In case of a hit, the

further exchange of information is regulated by legal provisions of the mutual judicial assistance.

Moreover, the treaty provides for automated access to the respective motor vehicle register. In addition, measures for the prevention of terrorist crimes and for fighting illegal migration are included in this comprehensive treaty.

In order to defend the citizens' interests which merit protection when exchanging/recalling personal data, comprehensive data protection regulations are laid down in the treaty. In addition to the mandatory general high data protection level, they also comprise the guaranteed purpose limitation principle when transferring personal data and regulations concerning the maintenance of data quality. Furthermore, the treaty provides for comprehensive technical and organisational measures related to data protection and data security, this includes mandatory documentation and logging when transferring data. Finally, all contracting parties foresee an independent control during data transfer by competent authorities whom the data subjects are entitled to consult in order to exercise their rights, among others the right to information. In Germany, the preparatory work for the ratification of this treaty already began in 2005; however, by the end of the year, it has not yet been concluded.

Greece

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Directive 95/46/EC

Directive 95/46/EC was incorporated into national law by *Law 2472/97 on the Protection of individuals with regard to the processing of personal data* (Official Gazette no A50/10-4-1997). A limited amendment of this law was adopted by art. 8 of Law 2819/2000 (Official Gazette no 84/15-3-2000), providing exemptions to the notification obligation for some categories of data controllers.

An English version of the amended text is available at www.dpa.gr

Directive 97/66/EC

Directive 97/66/EC has been implemented into national law by *Law 2774/99 on the Protection of personal data in the telecommunication sector* (Official Gazette no. A287/22-12-1999).

An English version of the text is available at www.dpa.gr

Directive 2002/58/EC

Directive 2002/58/EC has not yet incorporated into the national law. A special committee established in 2004 by decree of the Minister of Justice submitted a draft text to the Minister in September 2005. In March 2006, the Minister of Justice submitted to the Parliament a draft law for (a) the incorporation of the Directive 2002/58/EC into national law and (b) the revision of law 2472/97 on data protection in order to comply with the first report of the European Committee in regard with the implementation of the Data Protection Directive.

Main developments

There are no major developments to be mentioned under the first pillar.

Under the third pillar, Greece was evaluated in February 2005 within the framework of the competences of the Schengen Evaluation Group of the European Council. The evaluation of the HDPA, as the supervisory authority of the Greek SIRENE bureau, was performed on 8 and 9 February 2005, by a mixed group of DPA and police experts from Luxembourg (presidency), Belgium, Norway, Cyprus, Estonia and Sweden, with positive results.

B. Major case law

Guidelines for the safe destruction of personal data (1/2005)

The Hellenic DPA issued a text on Guidelines for the safe destruction of personal data after the expiration of the storage period which is necessary for the accomplishment of the purpose of the data processing.

According to the above Guidelines, data must be destroyed immediately after the end of the necessary storage period on the responsibility of the controller. In order to proceed with the destruction the Controller must adopt a written specific destruction procedure including mechanisms for the verification of the procedure application. In each case a Destruction Protocol must be drafted.

Specific reference is made on issues like destruction accomplished by the processor, destruction of data protected by special privacy codes etc.

Processing of sensitive data in TV shows

During 2005 two important cases were brought before the Courts. The first referred to a number of judges involved to corruption cases. The second referred to a number of clergymen, including bishops, involved to corruption and sex scandal cases. The cases were revealed during journalistic TV shows. The journalists had either used hidden cameras or proceeded to illegal telephone interceptions and made reference to the personal data of the persons involved or third persons. Some of these persons submitted complaints for illegal processing of their personal data.

The DPA judged that in the above cases the processing of sensitive personal data (projection during TV shows) can be justified due to the high public interest about the performance of public duties of public persons, if the disclosure is necessary to inform the public and constitutes a public interest but under the principle of analogy. This processing though is not justified if it concerns third persons not involved to the scandals. The repeated disclosure of this information can also be justified under certain circumstances, but this has to be judged in each case, also under the principle of analogy.

The DPA imposed a fine on the TV channels and the journalists for exceeding the analogy principle in some of the above cases and for the disclosure of personal data of third persons.

Publication of the Parliamentary Report on stock exchange transactions of the Members of the Parliament

Pursuant to a question submitted to the DPA by the President of the Parliament asking if the publication of the Parliamentary Report on stock exchange transactions of the Members of the Parliament, which is an act forbidden by the law, is in accordance with data protection law, DPA said that the publication of the Report is a processing that is permitted without the previous consent of the data subjects (Members of the Parliament) because it is necessary for the execution of a project of public interest which is executed by a public authority and obviously aims to achieve transparency in public life.

Publication of the names of persons who were illegally judged unable to serve in the army

The Minister of Defence submitted a question about the legality of the publication of the names of persons who were illegally judged unable to serve in the army in order to use it as a public example to avoid such phenomenon in the future.

The DPA said that the publication is not in accordance with the data protection law because it is not in analogy with the purpose of the Ministry's action which is to declare to the public that such phenomenon will not be accepted in the future. The DPA said that this purpose can be achieved with a more data protection friendly mean, which is the publication of the statistics on the number of cases that were examined and punished.

The case is pending before the Council of State where the Minister appealed the decision.

Use of CCTV in the city of Athens

By **Decision 28/2004** the HDPA gave the conditions under which the Hellenic Police had the right to install a CCTV in public areas of the city of Athens and its suburbs for the security of the Olympic Games 2004 until the end of the Games.

By **Decision 63/2004** the HDPA accepted the request of the Hellenic Police to extend for six months the period of lawful use of the CCTV, which expired after the end of the Olympic Games, only for the purpose of traffic management under strict conditions, among which the removal of microphones as well as of all those cameras which were installed in areas the monitoring of which was not justified for the purpose of traffic management and the obligation of switching-off the system during manifestations etc.

After expiration of the six-month period, the Hellenic Police requested the renewal of the CCTV operation period and applied for an extension of purpose in order to include the protection of persons and goods against criminal and terrorist actions (public security). In **Decision 58/2005 (12-8-2005)** the HDPA rejected the request for an extension of purpose, considering that the implementation of a global system of electronic surveillance is not in conformity with the principle of proportionality as it constitutes a serious violation of human rights to privacy and data protection without upgrading the citizens right to security.

The Minister of Public Order appealed the decision which is still pending before the Council of State.

C. Major specific issues

As the number of HDPA personnel (seven legal auditors and five IT experts) was very restricted and insufficient to fulfil its primary tasks properly, the Minister of Justice accepted the proposition for the recruitment of 14 more auditors (eight lawyers and six IT experts) as well as five more administrative staff. The procedure was competed in January 2006.

Hungary

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The Act on the Protection of Personal Data and Public Access to Data of Public Interest was amended and further refined in 2005. Most of the modifications had freedom of information implications. One modification concerned the regulation of "data for internal use and data connected to decision-making preparations", the definition of which was found to be insufficient, the use of which entailed the unnecessary and disproportionate limitation of freedom of information according to the decision of the Constitutional Court in 2004.

The Act refined the definition of data of public interest by clarifying that any record of information is to be regarded data of public interest irrespective of the way the data is processed, or the independent or collected character of the data. At the same time the right to access data of public interest cannot be restricted only in the interest of judicial but also of administrative authoritative proceedings.

Anyone may request the disclosure of data of public interest in whatever form (orally, in a written form, or electronically as well). The access to data of public interest published electronically cannot be made subject to registration. Only so much personal data can be processed which is necessary for fulfilling the request for disclosure including the payment of costs.

The Act on Freedom of Electronic Information passed by Parliament in 2005 provides for the obligation of publishing data of public interest and data public on grounds of public interest, thus making the procedure of legislation more open, making the digital version of the rules of law and the anonymised decisions of the Supreme Court more accessible.

The field of activity of the Commissioner of Data Protection has been widened. As of 1 June 2005 the Data Protection Commissioner represents the Republic of Hungary in the joint supervisory bodies of the European Union.

B. Major case law

In the recommendation on the data protection implications of the procedure of financial statement in accordance with the rules of the Act on Civil Servants, the Data Protection Commissioner stated that the aim of the introduction of the compulsory financial statement, i.e. to ensure the transparency of public life, could not be achieved by storing the financial statements of public servants and their family members. The storing of almost 300 000 financial statements harms the guiding principles of data protection, i.e. the principle of proportionality and the storing can be regarded as stocking, which had earlier been ruled unconstitutional by the Court of Constitution. Furthermore, the freely given consent of the family member who has to fill in his own financial statement is also questionable.

C. Major specific issues

The findings of an investigation concerning drug screening at workplaces show that drug screening at workplaces and the data controlling connected to it is not **generally acceptable** because:

- The voluntary nature of the consent of the employee is strongly questionable because

of the unbalanced positions of power between employers and employees

- Screening may lead to a practice seriously intruding into the privacy and personal rights

- The effectiveness of mobile testing is not convincing because test results provide information about the fact of consumption – or about physical contact with the substance – and not about aptitude for working.

The Data Protection Commissioner has summed up some points which shall be kept in mind in the legislative procedure.

A recurring topic in numerous countries in Central and Eastern Europe is revealing the past of former security agents. Draft legislation on the modification of the Archive Act was submitted by many Members of Parliament – by requesting but ignoring the Opinion of the Data Protection Commissioner at the same time. Their aim was to make it possible, by gradually extending the scope of the data accessible without anonymising and by disclosing, on the Internet, the documents to be protected from a national security respect, that the identities were revealed of all those who had co-operated with national security organs or who had been employed by these organs. The Commissioner made it clear that the proposal for modification does not meet the requirements of constitutional principles of data protection and, furthermore, it seriously violates people's right to privacy.

In another submission a citizen disapproved of his being obliged by his place of work to follow the precepts of the Church of Scientology and he had to fill in documents and questionnaires in which he had to disclose a wide range of personal data about himself and other persons. The Data Protection Commissioner of the Republic of Hungary is empowered to control each and all data collection in Hungary concerning personal data. This extends to the data collection of the registered churches as well. In his answer the Data Protection Commissioner called the attention to the following:

- everyone exercises control over his or her personal data and everyone decides whether to give his/her particular personal data to another person or not;
- if someone gives his/her personal data to the Church or to any organ of the Church, he/she may request to inspect his/her personal data collected and to have that data deleted as well;
- the person getting in contact with the Church or any organ thereof may exercise control only over his /her own personal data. He/she may exercise control over personal data of others if the data subjects have given their consent to it based on information provided prior to the data collection. If personal data of another person is transmitted to the Church or to any organ thereof without having obtained the consent of the data subject beforehand, the person transmitting the data is liable under civil and criminal law;
- every data controller is obliged, if the data subject requests information about the collection of his/her personal data, to give the requested information in an easy to understand way, within the shortest possible time, but not later than within 30 days from the lodging of the request;
- every data controller is obliged, on request of the data subject, with the exception of data collection ordered by an Act, to

delete personal data collected by him/her, according to the request of the data subject;
- providing the requested information or deleting personal data (with the exception of restrictions specified by an Act) cannot be refused by referring to any statement – signed either by the data subject or any other person.

The general director of a county hospital initiated an investigation on the health documentation of adopted children. The point was that all personal identifying data of the child changes following the adoption and by this, access to data of former treatments will be made impossible in the course of a later medication. Legal regulations in effect do not make connections between databases possible at present, but the constitutional right of the child to health is such an interest in a particular case that it may however justify the access to data related to former treatments and health condition kept by the health service provider. The factor 'worsening' the situation is that modification of data in health registrations has to be carried out so that the data modified remains readable. The Data Protection Commissioner initiated the amendment of legal regulations in his proposal sent to the Minister of Health and the Minister of Family Affairs, the essence of which is that the guardian authority may contact, by using registrations of the National Health Insurance Fund (NHIF – financing body), all health service providers that acted in the treatment of the child prior to the adoption, and may order them to delete old personal identifying data included in the health documentation and to change, modify the record with the new personal identifying data at the same time.

Ireland

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Both Directives have been fully transposed into Irish law. There were no legislative developments during 2005.

B. Major case law

The Commissioner successfully prosecuted a company before the Courts for a 'spam' offence under the terms of the Statutory Instrument that transposes Directive 2002/58/EC into Irish law.

The company was convicted in the Dublin District Court on five counts of contravening the law, in that it sent marketing messages to five mobile phones without the consent of the subscribers. The Company faced a potential fine of up to €3 000 per message sent. The Court imposed a fine of €300 per count (a total of €1 500). The Company was also ordered to pay costs of €1 000.

The prosecution arose from a number of complaints made to the Commissioner in March 2004 about a marketing campaign by the company that promoted a game of fortune by contacting mobile phones. In all cases, the mobile phone rang briefly and did not allow the complainants adequate time to answer before the call terminated. A 'missed call' was recorded and the phone listed a Dublin-based fixed-line number. When a person phoned that number, a pre-recorded message was played in which callers were invited to phone a premium rate number in order to avail of an offer to claim €50 credit for use in the game of fortune.

The Commissioner also made a number of individual decisions on complaints made under the terms of the Data Protection Acts, none of which were appealed to the courts. The most significant were:

- An individual complained that a CCTV camera used by the company operating the Dublin tramway system overlooked his back garden, giving rise to the feeling that the family were under constant surveillance. The company indicated that their policy in relation to CCTV was that cameras were to be used to monitor public areas and should not be used to monitor private areas. They acknowledged that the camera in question could indeed monitor parts of the complainant's back garden. The Commissioner indicated that the rules of data protection required that personal data recorded be relevant and not excessive for the purposes for which it was obtained. In relation to CCTV cameras, this meant that the camera must be positioned so that it could not capture non-relevant images in its vicinity. The company modified the system so that the monitor would show a blank screen when the CCTV camera moved over the private property in its range. The company indicated that these settings could not be changed by the personnel who were controlling the cameras in its central control room.

- A travel agency passed contact details of its customers to a credit card company which subsequently contacted some of these customers offering a 'co-branded' card (travel agency/card issuer). The booking form used by the travel agency indicated that information on the form was for use in fulfilling its contract with the customer and that information might be provided

from time to time to companies within the Group. As the credit card company was not a company within the travel agency's Group and as marketing a credit card is not the same as marketing a holiday, the Commissioner held that consent from customers should have been obtained prior to the marketing of the co-branded credit card. The company agreed to change its marketing practices to comply with the Commissioner's decision.

- A number of employees of a public institution submitted complaints that the biometric-based time and attendance system, involving central storage of data derived from fingerprints, constituted a disproportionate interference with their right to privacy. The institution indicated that the system had been introduced as part of a security review which took account of the duty of the institution to safeguard the valuable public assets in the building. It also referred to the security features built into the system, which ruled out use of the stored data to regenerate a fingerprint, and to the fact that the system had been introduced as part of a collective agreement with employees. The Commissioner decided that, in the circumstances, the system was proportionate and did not constitute an unjustified interference with the privacy rights of individuals.

C. Major specific issues

Community CCTV Schemes

The Commissioner was consulted by the Department of Justice, Equality and Law Reform on the data protection issues surrounding the proposed introduction of community-based CCTV schemes designed to deter criminal behaviour. The advice given to the Department was that personal data gathered by such schemes were covered by data protection legislation: it would be desirable that such schemes be put on a statutory footing, and that it would be helpful that their operation be covered by a Code of Conduct. In the course of the year, legislation authorising such schemes was approved by the Oireachtas (Parliament) and a Code of Practice covering data protection issues was published on the Department's website (www.justice.ie).

Italy

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Code of Digital Administration

In March 2005 the so-called Code of Digital Administration was enacted, consolidating several regulations including those related to electronic ID cards. The Code, also taking into account the Opinion rendered by the Italian DPA, specifies and indicates which data **must be** included in the electronic ID card (cardholder's name + tax ID Code) and that that **may be** included in the ID card.

Sensitive data may only be included at the cardholder's request. Apart from DNA data which are expressly excluded, the list refers to biometric data, blood group data, and the data on willingness to donate body organs in case of death.

The ID card can also contain other data useful for administrative purposes, in particular with a view to using electronic signatures. Additional specifications will have to be set out in ad hoc Regulations, especially with regards to biometric data.

There is no obligation for citizens to shift from their ID cards on paper to the new electronic ones, i.e. the scheme is managed currently on a voluntary basis.

Special care was taken in setting out the standards to be complied with for the production of the new electronic ID cards, including encryption and other security measures with a view to the storage of biometric data in the card's chip.

Urgent measures to fight international terrorism (Act no. 155/2005)

Following the attacks that took place in London in July 2005, the Italian Government issued urgent measures to enhance the prevention of and fight against international terrorism. Some provisions produce considerable effects on fundamental rights and freedoms, in particular the right to personal data protection:

a) Retention of telephone and Internet traffic data. Application of the provisions contained in the Data Protection Code concerning erasure of telephone and Internet traffic data was suspended until 31 December 2007, including unanswered phone calls.

Retention obligations were extended to Internet traffic data, for 12 months (six months for all purposes, plus six months for purposes related to terrorism and serious crime). On the measures required for implementing these provisions the DPA will have to render a prior Opinion.

b) Obligations applying to public phone and Internet access points. Whoever plans to make available terminal equipment for communication purposes to the public and/or customers and/or members (e.g. of a private club/association), including Internet-based communications, must get a licence from public security authorities. The owners and/or managers of the said access points will also have to monitor the activities carried out by their customers and store the relevant data, including customers' IDs. A decree by the Minister for Home Affairs, issued after consulting with the DPA, set out the specific implementing measures.

c) Coercive collection of DNA samples for identification purposes. The Criminal Procedure Code was amended by providing that the police may – failing the consent by the individual concerned – coercively collect hair and/or spit samples further to the written authorisation by the competent public prosecutor if this procedure proves necessary in order to identify any person that is the subject of specific investigations.

Prevention of fraud based on payment cards

In order to prevent fraud based on payment cards, Act no. 166/2005 provided for setting up a database at the Ministry of Economics. This database – which has not yet started operating – is expected to include, *inter alia*, the identification data of the merchants and the respective legal representatives where they have been disqualified from participating in the agreement with the credit/debit card issuer; in addition, the data of all the transactions challenged by card holders and other information related to fraud risk will be fed into the said database. Implementing rules will have to be laid down in order to detail the data and information to be specifically entered as well as the entities authorised to access the information, the access mechanisms in respect of the information contained in the database, and the data exchange mechanisms.

Electronic passport

Further to the EU Regulation setting out the requirements applying to electronic passports, on 29 December 2005 the Italian Ministry of Foreign Affairs issued a Decree on electronic passports after consulting with the DPA. The decree provides for inclusion of an RFID proximity chip in the passport cover, to store the image of the holder's face and the fingerprints of both his/her forefingers in interoperable format in addition to the information already contained in the paper document (data on holder, etc.). The biometric elements stored in the chip may only be used for the purpose of verifying authenticity of the document and the holder's identity via comparative elements that must be available directly, where the law requires submission of a passport and/or any other travel documents. The biometric data collected in order to issue the passport will not be stored in a centralised database.

B. Major case law

Constitutional Court – Decision no. 271 of July 17, 2005 – law-making power by regions

In an important decision adopted following a complaint lodged by the Prime Minister's Office against some sections of a regional law concerning measures to enhance development of the "information society", the Constitutional Court ruled that the said provisions were in breach of constitutional principles. The Court ruled that the measures in question impacted on the right to personal data protection and stressed that personal data legislation regulates several personal rights granted to each individual data subject, consisting of the power to retain control over the information concerning him/her and the mechanisms used to process such information. This is why this subject-matter falls within the scope of the competences entrusted to the State on an exclusive basis by Article 117 of Italy's Constitutional Charter. Regions may only take steps on a supplementary basis insofar as this is provided for by State-enacted legislation – for instance, they might be competent for regulating procedures or organisational mechanisms

envisaging the processing of personal data at regional/local level such as those related to establishment of an information network on regional facilities and structures.

Court of Cassation – 1st Division, Civil Matters – Decision no. 14390/2005

The Court of Cassation – which is the last-instance court in Italy's judicial system – granted the complaint lodged by a police official who had been suspended from office after he had been recognised in a hard-core picture on a website with "homosexual and feticist contents". The police official had lodged a complaint with the DPA against use of the sensitive data taken from the pictures, which had been posted on the Internet. He alleged the conduct of the police had been unlawful, in particular because his colleagues (who had found the addresses of the websites visited by the official at the latter's home and had subsequently proffered information on him) had acted outside their official duties. The Court – after the police administration (Ministry for Home Affairs) had challenged the decision by the DPA – ruled that dissemination of the data on the Internet does not mean that the data may be used without constraints. The data protection code actually safeguards publicly available and/or published personal data as well, exactly because any entity processing such data may derive an "informational added value" from them that is potentially capable of violating the data subject's dignity. Therefore, the data may not be processed insofar as it is publicly available, but rather to the extent that the relevant legal prerequisites are met. Such requirements would not appear to have been met by the Ministry for Home Affairs in the case in point, in particular considering that public bodies are expected to comply with more stringent safeguards if they are to process sensitive data, pursuant to the provisions set out in the law. Therefore, the Court ruled that the measure taken by the Ministry of Home Affairs against the police official was void and referred the case back to the competent court in order to establish whether the Ministry could lawfully process the highly sensitive personal data concerning the complainant.

Council of State – Decisions no. 4471/2005 and 5879/2005

The Council of State – which is the last-instance court as regards administrative law matters – issued two Decisions granting the right by municipality board members to access any records that may be helpful for them in discharging their duties. In particular, this access right also applies to documents and records (containing personal data on third parties) dating back to a period prior to the petitioners' term of office, because it is inherent in the discharge of their office with all its potential implications.

C. Major specific issues

In March 2005 the members of the collegiate panel of the *Garante per la protezione dei dati personali* were appointed by Parliament (for a four-year term); they are Prof. Franco Pizzetti (President), Mr Giuseppe Chiaravalloti (Vice-President), Mr Mauro Paissan, and Mr Giuseppe Fortunato. Mr Giovanni Buttarelli was confirmed by the new panel as Secretary-General to the Authority.

Public consultations: provisions adopted

Further to the outcome of the public consultations mentioned in the Eighth Annual Report, the Authority adopted four provisions of

a general character setting out safeguards and requirements in connection with loyalty cards, interactive TV, RFID devices, and videophones.

Loyalty cards and safeguards for consumers

The DPA set forth the measures data controllers were to take in order to ensure the lawfulness of their processing operations.

The principles can be summarised as follows:

a) Data Minimisation and Proportionality: information systems and software will have to be configured from the start in such a way as to minimise use of information relating to identifiable customers. Personal data related to customers may not be processed if the purposes of the processing – with particular regard to profiling activities – can be achieved by means of either anonymised data or indirectly identifying data; in particular, only such data as is necessary to award the benefits related to use of the card may be processed in connection with the loyalty programme as such.

b) Use for Direct Marketing Purposes: relevant, non-excessive data may be collected and used with a view to sending advertising materials, commercial communications, and direct selling. In principle, this only applies to the data that is directly related to identification of either the cardholder or his/her family members, or else of individuals specified by the cardholder. Use of personal data, if any, resulting from profiling activities must be the subject of a separate consent declaration by the entities concerned.

c) Information to Data Subjects: Customers must be provided with unambiguous, complete information (worded in a concise, colloquial style) before their data is disclosed and the card is issued, with a view to enabling fully informed adhesion to the proposed initiatives as also related to profiling and/or marketing activities.

d) Consent to the Processing: Consent is actually "necessary for the performance of obligations resulting from a contract to which the data subject is a party", therefore it is inappropriate to request it as if it were an option. Conversely, any other purpose of the processing that entails identifiability of data subjects – profiling and market surveys, or marketing activities – requires the data subjects' specific, informed consent as given separately for each purpose and provided in writing if sensitive data is involved. Subscription to the loyalty programme must not be made conditional upon the provision of the latter consent.

e) Retention Period: The principle to be abided by is that any personal data that does not need to be retained for the purposes for which it has been processed must be either erased or anonymised. In all events, the detailed data on the items purchased by identifiable customers may be retained for profiling or marketing purposes for no longer than 12 or 24 months, respectively, as to their storage, subject to their being actually anonymised in such a way as to prevent data subjects from being identified also indirectly and/or via interconnections with other databases.

Data protection and interactive (digital) TV

This provision has re-affirmed the principle whereby it is necessary to minimise use of information concerning identifiable users and subscribers and prioritise, in principle, anonymous data; secondly, it will be necessary

to refrain from collecting information that is not absolutely necessary – e.g., the titles of purchased movies must not appear in the relevant bills.

The use of pre-paid cards is favoured as a means to ensure users' anonymity. As for the billing of purchases, be they sports matches or movies, subscribers must have the possibility not to receive itemised bills – which should be provided exclusively on a specific request.

The provision stresses that it is unlawful to process personal data related to connection duration, viewed programmes and events, TV watching hours, watching interruptions, changing channels, and behaviour analysis in connection with TV ads.

If remote voting is used, which is often the case with TV shows, mechanisms will have to be implemented in order to keep the cast votes separate from the respondents' names. The same applies to market surveys and other sample-based surveys, where it is to be ruled out that personal data may ever be communicated to third parties.

Clear-cut, complete information notices are necessary, also in the light of the possibility for other household members to access the digital TV services, and the manner in which the data a user is about to provide will be processed must be specified in a mask to be displayed on the TV screen prior to the making of any purchase and/or the establishment of an interactive connection.

The data subject's consent will be required in order to monitor his/her choices and/or profile a subscriber; however, such consent must not be a condition to enter into the contract related to the other TV services.

As a rule, sensitive data may not be processed. It should be pointed out that the data subject's consent may also be given via the remote control device, whilst a specific password-restricted access will be necessary if consent is to be given to the processing of sensitive data.

Any information on subscribers may only be retained for a given period, which must be specified in the contract – the basic rule being that all data must be either erased or anonymised as soon as possible. Detailed data on purchases may not be kept for longer than 12 months; if the relevant contract is terminated, all the information must be erased within three months.

Safeguards applying to use of RFID devices

The requirements to be met in connection with the use of RFID devices were set out, also in the light of the Working Document issued in 2005 by the EU's Article 29 WP.

Basically, the provision requires both public and private data controllers to comply with the data protection principles set forth in the law, i.e.:

Data minimisation: in principle, RFID-based systems should be designed in such a manner as to avoid collecting personal data and/or making data subjects identifiable, except where this is absolutely necessary in view of achieving the purposes sought by the systems.

Information notice: individuals must be adequately informed of the presence and use made of RFID devices, including the presence

of RFID readers. This may require posting notices in the premises where RFID devices are used, however the information should also be available on the individual items bearing such devices.

Consent: private entities must get the data subjects' consent prior to using RFID devices if their use involves processing personal data; consent must be free and based on adequate information. If the devices are only used for payment purposes and no link can be established with identified and/or identifiable purchasers, then no consent is required.

Purpose specification: The data collected via RFID devices may only be used for the purposes for which it had been collected, and stored for no longer than is necessary. Individuals have the right to remove, de-activate and/or terminate operation of RFID devices upon purchasing a product bearing such devices. There must be user-friendly mechanisms available to do this. RFID devices should, as a rule, become inactive after a customer leaves checkout.

Additionally, specific provisions were laid down concerning use of RFID devices in the employment context and under-the-skin RFID implants, respectively. As to the employment context, it should be recalled that in Italy it is prohibited to deploy devices suitable for remotely monitoring employees; if RFID devices are considered to be necessary for controlling access to certain areas, the safeguards set out in the relevant labour laws and in the DP laws must be complied with.

As to under-the-skin implants, they are to be allowed only under exceptional circumstances (e.g. if it can be proven that they are necessary to safeguard the individual's health) because of their being in breach of the individuals' dignity (Section 2 of the DP Code) also pursuant to the Charter of Fundamental Rights of the EU. There must be the possibility for data subjects to have the RFID implants removed at any time and free of charge. Deployment of under-the-skin RFID devices is expected to be a matter on which prior checking by the DP authority will be required.

Videophones

The DPA set out the rules to be complied with in order to respect privacy and data protection in using videophones.

It was clarified that the data protection legislation does not apply if the videocalls are meant for personal use and the images do not go beyond the user's circle of personal acquaintances.

Conversely, if the images are disseminated, including via the Internet, the data protection legislation applies – which means that the data subjects' consent is required based on prior information. This also concerns third parties included in the images to be disseminated. Account must also be taken of the limitations possibly imposed on the use of videophones in public and/or private premises, which must be complied with to prevent the processing of data from being unlawful.

Additionally, the DPA called upon the manufacturers of videophones and the developers of related software to consider devising ad hoc functions to signal (e.g. via lighted indicators) that the videophone is operating.

Political propaganda and information to data subjects

On the occasion of the administrative elections and referendums scheduled in Italy in the first six months of 2005, and in view of the national elections in 2006, the DPA addressed several issues related to political propaganda in connection with data protection legislation via two ad hoc Decisions. Basically, political parties and movements, promoting committees, supporters, and candidates were exempted from providing information notices to data subjects if they processed personal data taken from publicly available registers, directories, records and/or documents exclusively for purposes of electoral propaganda and the related political communications, and the data subject had not been contacted by the entity using the data, or else received propaganda materials that did not allow information notices to be included easily (such as small leaflets or flyers as often used by political candidates).

In addition to this measure, the decisions re-affirmed the *decalogue* set out in a provision adopted in 2004, in which the principles and criteria to be abided by in political propaganda and communication were spelled out from a general standpoint. This provision set out:

a) The cases in which data subjects (i.e. citizens receiving political communications and messages) may be contacted without their prior consent – if the data is taken from sources that are truly "public", i.e. unlimitedly available to anyone, e.g. registers, directories, records and/or documents that are kept by a public body and can be accessed freely and with no limitations, as expressly provided for by a law and/or regulations. This category includes, basically, the so-called electoral registers, i.e. the lists of citizens entitled to vote as held by municipalities, the lists of members of professional rolls and councils, the data contained in some registers held by chambers of commerce, and other types of electoral register (e.g. the one concerning Italian citizens resident abroad). Conversely, it does not include, in particular, the data contained in the census register and the register of births, marriages, and deaths, which may not be supplied to private entities for electoral propaganda purposes – even if the applicant is a municipal administrator and/or the holder of an elective office.

b) The cases in which data subjects may only be contacted with their consent – which applies to all other cases where data is not taken from 'public' sources in the sense specified above, irrespective of whether SMS messages, MMS-systems, e-mail and other communication devices are used.

The DPA also pointed out that the obligation to provide an information notice is left unprejudiced if the data is acquired directly from the data subject rather than from public, freely available sources. A model information notice was drafted to be used in this connection.

Public Administration

Processing of Sensitive Data by Public Administrative Agencies

With reference to the processing of personal data performed by public entities, mention can be made of the Guidelines issued in April 2005 by the Minister for Public Administration, which recalled the obligation for public bodies to

adopt ad hoc privacy regulations on processing of sensitive and judicial data. The Italian DP Code (196/2003) allows public bodies to process sensitive and judicial data only if this is provided for by specific laws and/or regulations; however, if the latter do not detail the processing operations and data categories involved – which is usually the case – the individual public administrative bodies are required to set them forth via ad hoc regulations. This has not happened so far, and the Minister's Guidelines have set the framework within which public bodies are to adopt the relevant measures – which must rely on a careful assessment of the purposes pursued via the various processing operations as well as of the personal data that is actually required ('indispensable').

Additionally, the DPA issued a Provision (published in the Official Journal no. 170 of 23 July 2005) setting out the measures that are both necessary and appropriate for the processing of sensitive data by public data controllers to be in line with the data protection Code. Public administrative agencies are also required to spell out the personal information they collect and clarify how such information is used for the substantial public interest purposes referred to in the law. In order to facilitate compliance with these requirements, co-operation with the Prime Minister's Office, the Public Service Department, and the organisations representing Regions, municipalities and Universities was stepped up so as to draw up model regulations that can help streamline the safeguards afforded by other administrative agencies as well as simplify the process leading to adoption of the relevant regulations. Indeed, the latter must be adopted in pursuance of the DPA's Opinion, which is to be rendered within 45 days of receiving the corresponding request.

The DPA detailed the contents of the said regulations with particular regard to the following:

a) specifying the data that is indispensable (by category) in respect of the institutional activities to be performed

b) specifying the processing operations that are indispensable to pursue the substantial public interest set out in the law

c) providing an overview of the activities carried out by the public body concerned, with particular regard to the issues producing the greatest effects on citizens' rights. In this connection, public bodies should take adequate measures to ensure that the decisions made in respect of the processing of sensitive and/or judicial data are suitably publicised, availing themselves not only of their websites but also of targeted institutional communication initiatives.

On the whole, 33 regulations have been issued so far by public bodies – including, in particular, the Ministry of Environmental and Cultural Heritage, the Ministry of Defence, the Ministry of Education, and the National Research Council as well as several Chambers of Commerce, Regions, Municipalities and independent administrative authorities.

Revenue and taxation services

The DPA addressed several issues related to collection and use of personal data for the investigations carried out by revenue and taxation services under the law. In the light of the innovations brought about by the 2005 Budget Act to enhance the information-gathering

potential of the competent authorities, it was stressed that:

a) the exchange of personal data via electronic networks for banking investigations should take place in compliance with data minimisation and proportionality principles, i.e. by having regard to specific cases and targeted activities (no blanket collection of data is admissible);

b) rather than duplicating databases at the revenue service, the financial authorities should take steps to ensure that the required personal information can be extracted electronically from the existing public and private databases already containing such information;

c) specific safeguards should be implemented in using and retaining personal data contained in and/or extracted from the register of bank and savings accounts, out-of-court statements, and cadastre and mortgage registers (especially if the information is exploited for commercial purposes) as well as in respect of the electronic transmission of sick leave certificates to social security agencies.

Students' portfolio

The recently enacted reformation of the educational curriculum in Italy introduced a new tool for assessment and orientation called the 'student's portfolio', to be compiled by teachers in respect of the individual pupils/students. In addition to grades and educational reports, the portfolio is to include information on a pupil's/student's attitudes, expectations, and behaviour throughout his/her educational career.

The Authority pointed out the need to only include such personal data as is relevant and necessary to assess and orientate a student; sensitive data (medical data, data on psychological features, etc.), must only be included in the portfolio if it is indispensable for the assessment of the individual pupil/student. Each school will have to set out ad hoc measures to adequately inform parents and pupils/students about the portfolio and the data it contains, to enable parents to exercise all the rights granted to them under data protection legislation (access, rectification, etc.), and to adopt suitable security measures.

Providing healthcare by respecting human dignity

In a Provision adopted in November 2005, the measures to be adopted by public and private entities were laid down in order to bring the operation and organisation of healthcare facilities into line with the relevant provisions of the data protection Code, so as to ensure the best possible safeguards for individuals. Its main contents can be summarised as follows:

- Protecting Dignity
  It is necessary to always ensure the protection of an individual's dignity. This applies in particular to the disabled, children and the elderly as well as to patients undergoing invasive medical treatments and/or requiring special care (e.g. patients undergoing abortion).

- Protecting Confidentiality in Communications
  Healthcare staff must prevent the disclosure of medical information to third parties, in particular when making prescriptions or issuing certifications. This also applies whenever medical records (lab charts, health records, prescriptions) are to be delivered in

areas not specifically intended for this purpose (e.g. premises where several types of service are delivered, information counters, etc.).

- Queuing Distance
  Hospitals and healthcare bodies must set out an appropriate queuing distance as regards over-the-counter transactions (e.g. scheduling appointments) as well as when gathering medical information.

- Information Provided by ER Units/Hospital Wards
  ER units and hospital wards are allowed to inform, including by phone, whether a given individual was/is present within their premises, however this only applies to third parties lawfully entitled to obtain such information (relatives, friends and cohabiting persons). If the data subject is conscious and is not incapacitated, he/she must be informed in advance (e.g. upon being hospitalised) and allowed to decide who is to be notified of his/her presence in the ER unit/hospital ward.

- Waiting Rooms
  Patients should not be called up by their names when waiting for a given service and/or for being provided with certain records (e.g. lab tests). Alternative solutions should be implemented, e.g. by allocating a progressive number at the time a booking is made and/or a patient's application is registered.

- Lists of Patients
  Posting waiting lists of surgical patients in areas open to the public is not admissible, regardless of whether the individual diseases are also referred to.

- Information on Health Status
  Information on a data subject's health may only be provided to third parties if the data subject (or a relative, if the data subject is physically or legally incapacitated) has consented thereto specifically. On a case-by-case basis, other persons may provide such consent on the data subject's behalf (family members, cohabiting persons, etc.).

- Collecting Lab Tests
  Clinical reports, lab tests and certifications issued by labs and/or other healthcare bodies may be collected by individuals other than the data subjects providing they are entrusted with this task in writing and the information is delivered in a closed envelope.

Family doctors, private medical clinics and medical specialists are not required to take the above measures; however they must ensure respect for the data subjects' dignity and enforce professional secrecy obligations.

Public order

Numbered tickets and video surveillance in stadiums

The DPA was consulted with regard to two draft decrees submitted by the Ministry for Home Affairs to fight sports violence in stadiums, which envisaged the deployment of video surveillance systems and the issuance of numbered tickets.

As for video surveillance, it was found that its deployment was both lawful and necessary in the light of the acts of violence frequently taking place in football stadiums. The proposed retention period of image data, i.e. 1 week, was considered proportionate to the purposes

sought; however, if specific filming arrangements and techniques are to be used, they will have to be submitted to the DPA's prior checking.

Based on the information provided, there were no grounds to conclude that the proposed introduction of personal tickets was proportionate by having regard to the huge amount of personal data to be processed and the questionable usefulness of this measure for the purposes sought – as alternative control measures are available to identify violent fans and ban their access to stadiums. It was pointed out that if the competent authorities were to decide that personal tickets are necessary, they would have to specify the respective data controllers/processors, the retention period of the personal data, the entities authorised to access the personal information, and whether the data will be matched with that held by individual football associations.

Hotel registration information

In connection with a draft decree regulating anew the obligation for hotels and other accommodation facilities to send local police offices the identification data of all their guests, the DPA addressed a reasoned Opinion to the Ministry for Home Affairs. In particular, it was pointed out that:

a) there is no need for hotels and similar entities to keep the forms used for collecting their guests' data after the latter are communicated to law enforcement authorities, except for those required to comply with accounting and taxation obligations

b) the data may be communicated to police authorities either on paper or in electronic format; however in the latter case additional safeguards must be in place to certify the recipient's (i.e. the law enforcement authority's) digital identity

c) the data may not be included in a centralised database, as it must only be kept by the office of the local police; additionally, it will have to be kept separate from other types of personal data held by the police for public order/law enforcement purposes, and a short retention period will have to be provided for; more generally, it is necessary to re-consider need and proportionality of this measure in the light of the data protection Code. It is to be stressed that the Schengen Convention only envisages this measure in respect of non-nationals, and explicitly rules out that nationals' data should be communicated by hotels and similar facilities to police authorities. Additionally, this may only be done under the Convention if the data is necessary for the purpose of preventing or detecting criminal offences.

Telecommunications

In 2005, the provisions adopted in 2004 (see Eighth Annual Report) concerning telephone directories were implemented; accordingly, as for fixed telephony, 22 million users received the forms to specify whether and how their personal data and preferences should be reported in the printed or electronic directories. About 5 million users replied, of whom about 10% specified that they accepted to be contacted for marketing and commercial purposes. As for the rest, i.e. those that failed to reply, they will continue to be under the previous regime in accordance with the respective contractual agreements.

'Yellow Pages': Business telephone directories

In a Provision issued in July 2005, the criteria for compiling business listings such as *Yellow Pages* or similar directories were set out. In particular, no consent by the relevant business entities is required for the compilers and publishers of these directories to prepare the listings, as the information to be processed is related to the performance of business activities and is exempted, as such, from consent obligations under the law. However, data quality requirements must be abided by data being accurate, complete and updated. If the data is taken from the recently established 'unified database' (including all data on fixed and mobile telephony subscribers as well as holders of pre-paid card phones), all the accompanying preferences as listed in the database will have to be taken into account (e.g. it will not be possible to include the names of those entities that have opted out of being included in telephone directories). A simplified information notice to be used by the publishers of these listings was also drafted.

Interception of Communications

Following a wide-ranging and in-depth investigation carried out by the Authority between August and December 2005 in respect of the mechanisms whereby telecom operators comply with judicial requests to enable interception of communications, the findings obtained clarified that the operators do not access the contents of the interception and merely duplicate the communication line appertaining to the person under judicial investigation by routing the said line towards a telephone interception centre specified by the competent judicial authority. However, partly on account of the processing of personal data concerning both the person under investigation and third parties as well as of the additional services provided by telecom operators in these cases (e.g. geo-location of the relevant user, retrieval of data contained in the census register), some specific safeguards to be implemented when carrying out such operations were pointed out. They include organisational measures (reducing the number of the persons in charge of processing the interception data, separating accounting data from other data as produced during the interception activities); enhanced security (robust authentication procedures for the staff in charge of accessing the data in question, use of up-to-date technologies to communicate with judicial authorities by avoiding, for instance, facsimile communications, implementation of advanced encryption systems for as long as the data remained in the telecom operators' databases); and improved data protection (by erasing the data immediately it has been communicated to judicial authorities). Telecom operators were given six months to comply with these instructions.

Biometrics

Biometrics at the workplace

Following a prior checking request concerning the use of biometric data to control assiduity of a private company's employees, the DPA found that the planned processing was unlawful and banned its deployment. The decision concerned a building company with a staff of about 300, which was planning to use fingerprint data to control employees' assiduity, prevent some types of abuse, and overcome the problems caused by loss of magnetic cards; the collection of

fingerprint data was envisaged as a compulsory requirement for all employees, and the data would be subsequently stored in a centralised database.

Taking account of data quality principles, it was found that the envisaged mechanisms could not adequately ensure data reliability and integrity, in particular by having regard to accuracy in detecting both 'false negatives' and 'false positives'. By having regard to the proportionality principle, it was ruled that this kind of blanket use of biometric data was unlawful – partly because there are alternative mechanisms available to establish personal identity that are less privacy-intrusive, do not impact on personal freedom, and do not involve meddling with an employee's body. It was pointed out that it would have been preferable – if feasible - to store an identification code on a medium that remained at the data subject's sole disposal rather than store the said code at a centralised level in the company's information system.

Conversely, in a provision of 23 November 2005, the use of biometric data (fingerprints) was authorised to control and regulate accesses to a restricted high-security area within a plant producing defence technologies in the avionics and electronics sectors. The relevant company had submitted a request for prior checking, and the DPA ruled that the processing submitted to prior checking was lawful; this conclusion was grounded on the consideration of the specific purposes sought in the relevant context as well as of some precautions the company was planning to take in addition to those set forth by the Authority in respect of the concrete mechanisms applying to biometric identification.

Other Issues

Oblivion Rights

An important decision was made by the DPA in connection with a complaint lodged in 2004. The case had to do with the retrieval over the Internet of a decision issued by the Italian Antitrust Authority (which is not a judicial authority) against a company on account of misleading advertising; the said decision had been issued in 1996 and was subsequently posted on the Authority's website. The complainant alleged that the fact that the Decision was still available on the Internet whenever information concerning his current activities was being retrieved was in breach of his right to oblivion.

In the DPA's Decision, it was stated that the publication by the Antitrust Authority was lawful as it was provided for by the law, which however did not specify the detailed mechanisms of such publication; however, to ensure that the processing on the Internet was not in breach of data protection legislation, two measures were to be taken:

a) creation of a restricted-access section in the Antitrust Authority's website in which to post Decisions such as the one in question (dating back to 1996), which must not be retrievable by means of the standard external search engines

b) setting out by the Antitrust Authority of the period during which posting and free retrieval of a Decision on the Authority's website can be regarded as proportionate in view of achieving the purposes sought by the Decision in question.

It should be stressed that the Antitrust Authority complied with the Guidelines set out by the DPA; in particular, by applying the so-called "Robot Meta Tags" to certain pages (including the one containing the Decision at stake) the Authority prevented them from being retrievable by means of search engines. Additionally, the proportionate period for posting information on the Authority's website without any restriction – such as the one mentioned above – was found to be five years as based on the relevant antitrust legislation, whereby the sanctions to be imposed on repeated offenders are statute-barred after five years.

On the issues related to search engines and oblivion rights, the DPA adopted another Decision in November 2005 dealing, in particular, with the retention and availability on the Internet of newspaper articles dating back to several years before. The articles in question were no longer available on the website of the specific newspaper that had published them; however they could still be retrieved via Google – which showed, interestingly, the parallel processing carried out by Google by means of cache copies and the respective summaries.

Separate waste disposal

Having received several reports and claims alleging the violation of privacy rules deriving from the mechanisms implemented by some municipalities in connection with the separate disposal of solid waste and/or with detecting breaches of the relevant administrative rules, the DPA adopted a general provision setting out the measures data controllers were to take by having regard, in particular, to the proportionality principle. They include the following:

a) No transparent bags should be used in case of 'door-to-door' waste collection

b) No adhesive labels – including the data subject's name and address – should be placed on waste containers, in particular if the latter are located in a public street

c) Waste bags may be marked by a bar code corresponding to the holder's identification data; alternatively, they may be equipped with chip- or RFID-based tags

d) The competent inspection bodies may not carry out blanket inspections of the waste bags; such inspections should be performed selectively and only if there are grounds to believe that the waste has been disposed of in breach of the relevant legislation/regulations and there is no other means to identify the alleged offender(s)

e) Names and addresses of the citizens taking their waste to the so-called *ecopiazzole* (environmentally friendly waste disposal areas) for separate waste disposal purposes may be lawfully recorded, albeit on a transient basis.

Taxicabs and customers' data

The requirements to be complied with by companies managing cab reservation services (so-called 'radiotaxi' services) were spelled out. These companies usually request customers' data at the time of reservation to provide their services, and the Authority recalled the criteria to be abided by in this regard following several complaints also lodged by consumer associations – whereby some companies were said to also store additional information related to customers' behaviour (e.g. no-show cases,

provision of wrong address, failure to pay a fare) without informing them. Such information was allegedly used by the companies to decide whether to provide their services in future to that specific customer.

It was stressed that such additional information may not be collected and stored by the companies in question, which should limit themselves to only acquiring such data as are necessary to get in touch with the customer and establish his/her identity as the person actually making the relevant reservation (e.g. home address or phone number). This data must be erased upon conclusion of the fare, except in specific cases (e.g. disputes on the price paid for the fare, returning of lost objects) – whereby the maximum retention time should not be in excess of 30 days. Companies must inform customers of the mechanisms and purposes of data collection prior to proceeding with the reservation procedure (e.g. via a pre-recorded standard message), and request customers' explicit consent to use their data for the purposes of marketing and/or market surveys.

Credit factoring: need to respect the persons' dignity

In order to bring the processing operations related to credit factoring into line with the provisions in force concerning personal data protection, the necessary measures to be taken by the relevant data controllers (or any third parties acting on their behalf) were specified. In particular, it was recalled that the processing must be lawful (no disclosure of the debtor's data to third parties without justification, e.g. to put pressure on him/her; no use of pre-recorded telephone messages without operator's intervention to urge payments) and fair (no posting of mail cards bearing "credit factoring" labels, no dissemination of data to third parties by using similarly marked mailing envelopes); additionally, only such data as is necessary for the specific factoring purposes must be processed (e.g. name, place and date of birth, tax ID code, amount at issue), and the data must be erased upon conclusion of the factoring activities (i.e. upon levying the relevant debts). It was also pointed out that data subjects may challenge under the competent judicial authorities if the conduct followed in connection with credit factoring qualifies as an offence under either civil law (as regards claiming damages for the harm suffered, if any) or criminal law (if the conduct amounts to a criminal offence such as harassment or threats).

Enforcement

Special attention was paid to enforcement activities throughout 2005. This applies, in particular, to the enhancement of inspections and investigations in several sectors ranging from the use of loyalty cards to credit reference agencies, telephone traffic data retention, personnel recruitment, and the processing of personal and sensitive data by healthcare agencies.

Two hundred and fifty on-the-spot inspections were carried out in 2005 all over Italy. About 100 breaches of data protection laws were found and the relevant fines were imposed. This was made possible, *inter alia*, by an ad hoc Memorandum of Understanding between the *Garante* and Italy's Financial Guard – a police corps in charge of supervising compliance with taxation and financial legislation in Italy. Based on this Memorandum, the DPA may avail

itself of staff from the Financial Guard to carry out inspections (under own instructions) in particular at peripheral level.

Among the most important inspection activities, reference can be made to the investigations performed in respect of allegedly unlawful accesses to the computerised registers of the Municipality of Rome (census, register of births, deaths, and marriages, etc.), which are managed by a company controlled by the Latium Region (of which Rome is the capital). This inspection showed that staff from the company in question had infringed data protection obligations (in particular, by unlawfully accessing personal data of candidates to regional elections and failing to comply with the allocation of tasks required under the law). Additionally, the Authority pointed out the need to amend the Memorandum of Understanding regulating the relationships between Latium Region and Municipality of Rome to prevent direct online access by regional bodies and agencies to the registers held by the municipality, which, in turn, will have to upgrade security measures and technical arrangements applying to such registers and develop a "push" system to forward the data to the applicant entities. The Provision issued by the Authority was published in the Official Journal of the Italian Republic, as the requirements set out in the specific case are actually applicable in broader perspective to all local municipalities.

Latvia

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Amendments to the Personal Data Protection Law

To ensure the conformity of legal acts of Latvia to the requirements laid down in Directive 95/46/EC and to establish the basic principles of the work of the institution that supervises personal data, the Prime Minister established a working group, on 10 January 2005, whose task was to prepare the relevant draft legal acts. The draft law, Amendments to the Personal Data Protection Law, was prepared. The purpose of the draft Law is to specify the personal data processing systems to be notified and the procedure of notification, to specify legal norms that have caused problems in the application of the Law, and to specify the requirements of Directive 95/46/EC implemented in the Personal Data protection Law, including those in relation to the legal status of the State Data Inspectorate.

Simultaneously, Amendments to the Satversme (Constitution) of the Republic of Latvia have been prepared and the adoption thereof is related to the legal status of the State Data Inspectorate.

During discussions, an agreement on a draft Law that stipulates that an exception to the general principle that all state administration authorities are subordinate to the cabinet of Ministers has to be specified at the level of the Constitution was reached. A possibility was provided in the Constitution to stipulate that an authority may not be included in the state administration hierarchy system. Section 58, paragraph 2 will stipulate, "The Saeima (Parliament), in order to ensure appropriate administration, may specify the authorities that are not subordinate to the Cabinet. The competences and structure of such authorities shall be stipulated by an individual law." The first sentence of paragraph 2 stipulates that the Saeima, in compliance with the law, may establish authorities that are not functionally and/or institutionally subordinate to the Cabinet. The words "that are not subordinate to the Cabinet" comprise two possibilities:

1) To stipulate that an authority is not subordinate to the Cabinet functionally, i.e. as to decision making, while remaining institutionally subordinate to the Cabinet, e.g. in relation to disciplinary liability, finances, work organisation, etc. In this case the authority is under the administration of a ministry. The contents of administration are stipulated by the law,

2) To stipulate that an authority is subordinate to the Cabinet neither functionally nor institutionally.

The second sentence of Section 58, paragraph 2 stipulates, "The competences and structure of such authorities shall be stipulated by an individual law." If a decision is made to release some authority from the subordination to the Cabinet, the Saeima will do so by an individual law each time, laying down in the law the structure and competences of the authority. Depending on the type of authority, a different solution could be used in each individual case.

There is no plan to adopt a common 'umbrella' law on all independent authorities. An individual law will be adopted by each authority. It is justified, because the authorities to be released form the subordination to the Cabinet are very different and, therefore, an individual and specific

law in accordance with the actual circumstances is required. The legislator may not assign a "smaller independence" to an authority than is necessary for appropriate administration in the particular state administration field, and neither may it assign "superfluous independence" to an authority in fields where it is not necessary (namely, the authority is able to perform its tasks also if subordinate to the Cabinet) or if it will not ensure appropriate administration.

An individual law will stipulate the legal status of an authority, its subordination, and procedure of establishment, functions, financing, and other matters. The reference included in Section 58 of the Constitution stipulates also a totality of a number of specific measures:

1) independence guarantees to senior officials of authorities

2) ex-ante and ex-post controls of adopted regulatory acts, as well as other measures to ensure lawfulness and usefulness

3) authorisation to issue specific external regulatory acts.

On 23 February 2006, the draft Law on the amendments to the Satversme of the Republic of Latvia was submitted to the Cabinet of Ministers. Following the adoption of the Law on the Amendments to the Satversme of the Republic of Latvia by the Parliament, the preparation of other required regulatory acts will be coordinated by the Ministry of Justice. In addition, the draft laws "Amendments to the Administrative Procedure Law" and "Amendments to the Law on the Procedure of Announcing, Publication, Entering into Force and Validity of Laws and other Acts Adopted by the Saeima, the President, and the Cabinet of Ministers" will be prepared.

Amendments to the Criminal Law

At present, administrative liability is stipulated for violations in the processing of personal data – warnings, cash penalties, suspension of personal data processing system and forfeit of the technical means used.

In order to facilitate the protection of personal data processing and to prevent illegal personal data processing, the work on stipulating criminal liability for violations in the processing of personal data began in 2005. The draft Law will be submitted to the Cabinet of Ministers in the first half of 2006. The draft law stipulates criminal liability for illegal personal data processing if it is performed repeatedly within one year, as well as if it has been performed by a group of persons upon previous agreement; for the said activities if they have been performed in order to take vengeance, blackmail or with other purpose, or if it is connected with violence, fraud or threats; for not using the required technical and organisational means to protect personal data and prevent illegal processing thereof resulting in a substantial damage incurring; and for illegal processing of personal data resulting in a substantial damage incurring.

Amendments to the Electronic Communications Law

The Law was adopted by the Parliament on 12 May 2005. The law specifies the provisions of Directive 2002/58/EC, for example, in relation to the processing of traffic data, location data, and publicly available lists of subscribers.

Amendments to the Information Society Services Law

The Law was adopted by the Parliament on 10 November 2005. The Law specifies the legal

norms in relation to the prohibition of sending commercial communications by implementing Article 13 of Directive 2002/58/EC, and it specifies the supervision authorities in relation to the circulation of information society services, inter alia the State Data Inspectorate, which carries it out within the scope of its competence.

B. Major case law

The complaints received by the State Data Inspectorate and the inspections carried out by it show that in 2005 the majority of violations of the Law were connected with personal data processing without any legal base.

Most typical violations of personal data processing were:

1) incorrect and often explicitly illegal personal data processing in the collection process of loans (credits) and payments overdue (black lists)

2) non-informing of data subjects and refusals to provide information to data subjects (especially in medical services)

3) disproportional personal data processing, exceeding and expanding the initial purpose for data processing.

C. Major specific issues

Accessibility to court judgments

The accessibility to court judgments was widely discussed in relation to the development of the Common Court Judgments Database (and the portal www.tiesas.lv) in Latvia and data availability on the Internet.

Freedom of information and data protection

Availability of data on state officials' declarations on the Internet. Publicising of the income and premiums received by state officials. Publicising of data on receivers of rural support payments. Publicising of names of malevolent violators of traffic rules.

Research of human genome

Considering that a common human genome research database, which is intended for data processing for scientific purposes, is being developed in Latvia at the moment, the State Data Inspectorate carried out an inspection at the genome database of the Biomedical Research and Studies Centre of the University of Latvia. The inspection and the statement from the State Data Inspectorate is a pre-condition for commencing the processing of human genome in Latvia.

Protection of patient rights in relation to compliance with the rights of data subjects

The Law on the Protection of Patient Rights was prepared, and it contains a number of norms that specify the rights of data subjects in the sphere of medicine.

Data protection in labour relationships

The State Data Inspectorate prepared the Recommendations on Personal Data Protection in Labour Relationships. The handbook is intended both for employers and employees, and it explains what personal data may be processed by employers and whether they must inform their employees about the data processing performed.

Lithuania

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

1. The Law on Electronic Communications of the Republic of Lithuania assigned to the State Data Protection Inspectorate control of enterprises providing electronic communications networks and/or services in respect of their compliance with the requirements of paragraph 1 of the Article 63 of the aforesaid Law concerning confidentiality of communications. Enterprises providing electronic communications networks and/or services shall create conditions for the State Data Protection Inspectorate to carry out the control activities provided for in paragraph 2 of the Article of the aforesaid Law in accordance with the procedure established by the Government. On these grounds, on the 20 July 2005 the Government of the Republic of Lithuania passed the Resolution No. 807 approving the Rules on performing inspections of communications confidentiality. This resolution determines the procedures of the inspections carried out by the State Data Protection Inspectorate concerning compliance with the requirements of paragraph 1 of the Article 63 on confidentiality of communications, and of the production of inspection results.

2. Pursuant to the Law on Electronic Communications, the State Data Protection Inspectorate prepared the Requirements for the itemised bills which were approved by Order No. 1T-95 of 5 July 2005 of the Director of the State Data Protection Inspectorate. It mentioned requirements to determine the content of itemised bills issued by providers of publicly available electronic communications services and their forms produced to the subscribers of publicly available electronic communications services.

3. On 7 December 2005 the Government passed Resolution No. 1317 "On the Amendment of the 20 February 2002 Resolution No. 262 of the Government of the Republic of Lithuania "On the Reorganisation of the State Register of Personal Data Controllers, Approval of the Regulations of the Register and of the Procedure of Notification by Personal Data Controllers of Processing of Personal Data". This resolution establishes the simplified procedure of notification of processing of personal data and relates to the procedure of carrying out prior checking laid down in the Law on Legal Protection of Personal Data and the procedure of registration of data controllers.

B. Major case law

The State Data Protection Inspectorate performed the inspection at an agency that used a stationary system of measurement of speed and the registration of red light violations (TraffiPhot) for the purpose of testing the efficiency of the operation of the system. When triggered, the system took photographs of drivers that exceeded the speed limit or were driving through the prohibited - red signal of the traffic light. This data was automatically transferred to the Lithuanian Police Traffic Supervision Service. It was possible to identify the drivers with the help of a video database of drivers. These photos were then made public on TV. The State Data Protection Inspectorate established that an administrative offence had taken place since the agency processed personal data by automated means without

prior notification to the State Data Protection Inspectorate and the agency had not informed the data subjects about the processing of the personal data. In its Decision the court stated that the information recorded by cameras and video surveillance, by which the person might be identified, was considered as personal data. Therefore the provisions of the Law on Legal Protection of Personal Data were applied for the processing of these video data. The court did not impose a fine on the director of agency as the agency collected personal data legally and for the purposes of the introduction of the TraffiPhot system. In its Decision the court indicated that presently the standard of driving might be assessed as low in Lithuania. Due to the violation of the traffic rules many accidents occurred resulting in a lot of deaths and injuries. It was necessary, therefore, to take measures to discipline drivers as this could possibly prevent violations of traffic rules and allow for quick investigation of traffic accidents. Technical measures such as the TraffiPhot system ought to be in service to achieve these purposes. With regard to testing the TraffiPhot system, the offenders were recorded committing traffic violations that could have serious consequences and this means that, under the proportionality principle, the violation in the field of data protection was assessed as less critical than the serious traffic violations committed which were recorded by the TraffiPhot system.

C. Major specific issues

Problems of personal data processing for historic purposes

Since the Law on Documents and Archives came into force on 1 January 2005, people carrying out historical research have been faced with the problem of accessibility to documents. In compliance with the Law on Documents and Archives, access to the documents of the National Documentary Fond, which contains information on a person's private life, as well as to structured sets of personal data, transferred to state archives, shall be limited for a period of 50 years after the person's death, and in the event of failure to establish this fact for a period of 100 years after the creation of said documents. Consequently certain problems occurred of how historical research should be interpreted, since the Law on Legal Protection of Personal Data does not foresee any specific provisions on the carrying out historical research although it does determine provisions on carrying out scientific research.

In accordance with the Law on Legal Protection of Personal, personal data can be processed if the people carrying out scientific research obtained the data subject's consent. Without the data subject's consent personal data may be processed for the purposes of scientific research only if the State Data Protection Inspectorate, which must carry out a prior check, has been duly notified. To resolve this issue with regards to historical research, meetings were organised with the representatives of Department of Archives and various historians in order to resolve the emerging problems. As a result, the State Data Protection Inspectorate prepared a recommendation on the processing of personal data performed during historical research. The purpose of this recommendation is to outline the basic rules on how personal data can be processed during historical research in order not to violate the data subject's right to privacy, and to ensure secure and lawful processing of personal data. Also the State Data Protection Inspectorate prepared the recommendation on filing the form of notification for prior checking

while processing personal data for the purposes of historical research.

The security of sending bills of providing services

A registered lobbyist in Lithuania approached the State Data Protection Inspectorate due to the fact that the public utilities companies sent the notifications about providing services to customers by clear text. To help data controllers ensure compliance with the provisions of the Law, the State Data Protection Inspectorate prepared the recommendation on the protection of personal data when sending bills for services. The recommendation states that the bills for services cannot be produced publicly (for example, putting the bills on the notice board) and the data controllers have to ensure the bills are doubled over and sealed in an envelope.

Cases on the use of personal identification number

The personal identification number (PIN) is a unique sequence of digits assigned for a person's identification, collection of data about him, and ensuring of interaction between state registers and information systems. The PIN assigned to a person is unique and unalterable. Frequently data controllers collect PINs from data subjects not for the purpose of identification but in order to keep this data although it is not used for any other purposes. For instance, the State Data Protection Inspectorate receives more and more complaints from people on shops collecting their PINs while changing or returning goods of inadequate quality. After examination of complaints, the State Data Protection Inspectorate detected that data controllers have been processing excessive personal data in the form of the PIN, because this is not necessary for the purposes for which they have been collected and are not used for any other purpose.

Having performed inspections concerning the processing of PINs for direct marketing, the State Data Protection Inspectorate gave instructions to data controllers, such as credit unions and banks, not to collect and further process data subjects' PINs for direct marketing and to stop the processing of PINs which were collected for other purposes.

The Government turned the State Data Protection Inspectorate's attention to the information provided in the press about forthcoming public sales. The State Data Protection Inspectorate checked the information which was on the Internet and determined that producing the information about forthcoming public sales the bailiffs provided excessive data about the owners of estates for sale (such as a personal identification number, a date of birth, an address). The bailiffs were instructed not to advertise this excessive personal data of owners of estates being sold by public auction.

State and departmental registers

In 2005 the State Data Protection Inspectorate performed inspections at state institutions, which possessed state or departmental registers containing personal data, in order to determine what information was being provided from registers, to whom it was being disclosed and whether the data disclosure contracts were concluded lawfully. After checking most of the registers, no infringements of the Law on Legal Protection of Personal Data were detected. In two cases, however, the state institutions were instructed to ensure the compliance of the provisions of the above-mentioned Law.

The conference 'E-commerce and data protection'

In dealing with the development of the information society in Lithuania, the protection of personal data acquires greater significance. The Internet and the opportunities offered by it involve more and more public activity spheres, increasing the scope for personal data to be collected and processed on the Internet. In electronic space a person tends to be especially perceptible, thus his personal data might become more vulnerable.

With the rapid changes of information technologies, specific problems arise: how to facilitate favourable conditions for electronic business development and also to ensure the right to inviolability of one's private life. The ways and means of achieving such compatibility, to strengthen society's confidence in data controllers, to create secure space on the Internet and tackle the threats that appear were considered during the conference 'E-commerce and data protection', which took place on 14-15 November 2005 in Vilnius. Other issues covered during the Conference were e-commerce and privacy policy; direct marketing and data protection; organisation of data protection within the company; good practice in processing personal data within international companies; identification on the Internet; the fight against spam; cybercrime; e-banking and fraud.

PHARE project

From 29 March 2004 till the end of June 2005, the State Data Protection Inspectorate together with the Ludvig Boltzman Institute of Human Rights (Austria) carried out the PHARE programme twinning project LT02/IB-JH-02/03, "Strengthening administrative and technical capacity of personal data protection".

On 30 June 2005, the PHARE project was completed. As part of this project, specialists from the State Data Protection Inspectorate had traineeships at the Independent Centre for Privacy Protection in Schleswig-Holstein, the Data Protection Commissioner's office in Bonn, in Germany, and in the Bureau of the Data Protection Commission in Vienna, Austria. During the traineeships the specialists from the State Data Protection Inspectorate learnt about the procedures of executable inspections and about handling complaints, and they participated in on-the-spot inspections. It is also worth mentioning that during the PHARE programme twinning project a Commentary to Law on Legal Protection of Personal Data of the Republic of Lithuania was prepared. This Commentary will be very helpful in understanding the provisions of Law to data subjects and to data controllers, to state and municipal institutions and enterprises (for example, it would be especially useful to judges enabling them to fairly interpret and apply the provisions of Law on Legal Protection of Personal Data of the Republic of Lithuania), and to private institutions (enterprises).

Luxembourg

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Law of 2 August 2002 regarding the protection of persons with regard to the processing of personal data

The *Commission nationale pour la protection des données* has advised the government concerning the planned modification of certain provisions of the framework data protection law (Draft law No. 5554 of 16 March 2006), especially concerning the simplification of those formal requirements which are not considered as essential for the protection of the freedom and fundamental rights of citizens. Furthermore, several minor points have been clarified and the scope of application of the law has been restricted to natural persons

After its adoption by Parliament in 2007, the future modified law will provide for more extensive exemptions from the notification requirement and certain data processing will no longer be subject to "prior checking" (authorisation by the CNPD).

Law of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications (implementation of Directive 2002/58/CE)

This law was adopted by Parliament on 30 May 2005 and entered into force on 1 July 2005.

Following a recommendation of the *Commission nationale pour la protection des données,* the government intends to reduce the duration of the mandatory data storage and retention period applicable to traffic data of electronic communication services from twelve months to six months.

Law of 8 June 2004 regarding the freedom of expression in the media

The above mentioned draft law of 16 March 2006 will also fit the wording of the law of 8 June 2004 concerning the respect of freedom of the press and the liability and obligations of editors and journalists to the modified rules of the data protection law of 2002 as the press council and the representative bodies of journalists and publishers will have to include the rules of data protection in their professional code of conduct. The enforcement of these rules will then have to be monitored continuously by the committee for press complaints as a self-regulation for professionals of the Press and Media sector.

Decrees and secondary legislation

A regulation has been adopted (30 September 2005) in accordance with the Data Protection law for the determination of such natural or legal persons authorised to process health data for the purpose of preventative medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, or scientific research in the field of biology and medicine.

Other legislative developments

In April 2005 the Government requested the opinion of the CNPD on a draft law regulating access by judicial and police authorities to personal data processed by the State administration and by public authorities.

The CNPD advised the Government to adopt a more restrictive approach and a better implementation of the rights of concerned persons.

The CNPD also took the position on proposed regulations for an automated system of the monitoring of travellers by accommodation operators and made several suggestions for improvement of the draft.

A draft law was brought before Parliament on 15 November 2005 for approval of the Treaty of Prüm, signed between seven Member States on 27 May 2005, enhancing cross-border Police co-operation, in particular to combat terrorism, cross-border crime, and illegal immigration. It also modifies the law of 21 December 2004, which approved the Treaty signed on 8 June 2004 in Luxembourg regarding trans-border police intervention.

B. Major case law

Civil and criminal case law

There are still no significant Court decisions to report regarding general questions of Data Protection, as well as in civil as in criminal matters. However, as the DPA's Decisions regarding authorisation of data processing subject to prior checking can be challenged before the Administrative Courts, some case law was developed in that field.

Administrative case law

On 23 February 2005, the Administrative Court of Luxembourg overruled a decision of the *Commission nationale* which had limited to a period of two weeks the time during which the tape records may be stored by a jewellery shop put under video surveillance with authorisation of the CNPD. The Court considered that this period was too short, especially in order to allow due consideration by the police in case of investigation into preliminary preparations of a later hold-up.

On 9 May 2005, the Administrative Court overruled a decision of the *Commission nationale* which had ruled that Public administrations were not to be considered as "enterprises" in terms of Article 11. The Law limits the eligible purposes for setting up surveillance of the workforce by the employer to those enumerated by law, among those Article 11 paragraph (1), b), with the aim of protecting goods and properties of the "enterprise". This means that administrations can also carry out surveillance on the workplace in order to protect their property.

On 12 July 2005, the Administrative Court of Appeal confirmed a judgement of 15 December 2004 of the Administrative Court which had rejected the request for cancellation of a decision of the *Commission nationale* forbidding video surveillance in a shoemaker's store.

On 8 November 2005, the Administrative Court of Appeal confirmed the above-mentioned decision of 23 February 2005 of the Administrative 1st degree Court.

C. Major specific issues

The *Commission nationale pour la protection des données* issued its first decision in a case of biometrics. The Commission refused to authorise the use of a biometric system for access control in a Wellness and Fitness Centre. The Commission ruled that the storage of biometric data in a

central database by the operator was excessive in relation to the purpose of controlling the access of registered subscribers of the Wellness and Fitness Centre.

In another case the *Commission nationale* did not grant authorisation for the communication of personal data from the national social security administration to a public survey institute which intended to use the data to determine a sample of persons to be questioned as a representative sample of the population. In the specific case the scientific aspect of the planned study was not deemed to have been given in order to justify the application of Article 6 § (1) letter b second sentence which allows further processing if needed for scientific, statistical or historical purposes.

Along with the competent public authorities, the *Commission nationale* has taken part in the preparation work (concerning both technical and practical aspects) in view of the forthcoming introduction of the biometrical passport in Luxembourg (due in August 2006).

In addition, the *Commission nationale* has discussed and co-operated with the governmental authorities presently preparing action plans concerning e-health and e-government, as well as a report for a strategy of simplification of administrative procedures and burden imposed on private enterprises. In the next two years the activities of the Commission nationale will focus to a large extend on these matters.

A significant number of experts have submitted applications in order to obtain the CNPD's approval for their appointment as data protection officials by data controllers. The *Commission nationale* granted them guidance and training by means of workshops.

The *Commission nationale* continued its information and awareness raising campaign by publishing a calendar with a consumer support association.

An information booklet, already published with the support of the Governmental Information and Press department in 2004 in German, French and English, was also made available in 2005 in Portuguese.

The DPA's website has been relaunched successfully and now offers an improved layout and additional contents (dossiers). A well-known financial and economic magazine has even designated it as "website of the month".

Video surveillance operated by the police in public spaces and the use of genetic data for the identification of persons in the domains of law enforcement and criminal law were the most relevant topics commented on by the press during the past year.

Malta

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The EU Data Protection Directive 95/46/EC was incorporated into Maltese Law under Chapter 440 by Act XXVI of 2001 as amended by Act XXXI of 2002 and Act IX of 2003. The Data Protection Act was fully brought into force in July 2003, establishing the obligation of notification by July 2004. Certain provisions relating to manual filing systems will be effective from October 2007.

Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, was incorporated by Legal Notice (L.N.) 16 of 2003 and L.N. 19 of 2003 both brought into effect in July 2003.

Other legislative developments:

During 2005, L.N. 16 of 2003 was amended so as to extend the applicability of the provisions relating to unsolicited communications also to legal persons as well as natural persons.

B. Major case law

None to report

C. Major specific issues

Developing Guidelines

In terms of Article 40 of the Data Protection Act, the Data Protection Commissioner regularly met representatives of the various sectors with the objective of discussing and agreeing on principles emanating from the Act and then to articulate them in the form of Guidelines or codes of practice.

➔ Education
Data protection Guidelines on the processing of visual images in schools have been launched in October.

These Guidelines, the first in a series, have been jointly developed by the Commissioner and a committee of school representatives composed of representatives of state schools, independent schools, church schools, the Education Division and the Office of the Prime Minister. The Guidelines are intended to define good practice to be adopted in schools.

➔ Insurance
A working group composed of representatives of the Malta Insurance Association, the Association of Insurance Brokers, the Malta Financial Services Authority and the Office of the Commissioner regularly met to discuss data protection issues within the sector.

Topics discussed included the procurement of consent, the obligation to provide information, the right of access, and the sharing of information for the prevention of insurance fraud. Best practice procedures were identified for each topic with the intention of including them in published Guidelines.

The working group will keep on meeting to discuss further issues specific to the insurance sector such as the collection of medical data of hereditary nature relating to relatives of applicants and retention periods.

➔ Banking
Guidance notes to be used internally by banks have been developed in conjunction with the Malta Bankers Association. The contents of these guidance notes will be the basis of Guidelines which will be issued in the future by the Data Protection Commissioner and which will be directly intended for data subjects.

➔ Security
Surveillance methods involving the collection and other processing of personal data, is another sector where Guidelines will be issued by the Office. Meetings with representatives from the sector have focused on CCTVs.

Twinning light project

In October 2005, a 'twinning light' agreement was signed with the German Federal Commissioner for Data Protection. Both this Office and the central directorate on data protection within the Office of the Prime Minister can avail themselves of the expertise of the short-term experts who come over to deliver their assignments in the various sectors.

The main objective of this project is to assist the Commissioner to strengthen and consolidate the resources and expertise required to fulfil his duties and obligations in the administration and enforcement of the Data Protection Act.

The Netherlands

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Directive 95/46/EC was incorporated into national law by an act of 6 July 2000[21] and entered into force on 1 September 2001, replacing the old data protection law, the *Wet persoonsregistraties (Wpr)*, which dated from 28 December 1988.

Directive 2002/58/EC has been incorporated into Dutch law mainly by the changed *Telecommunicatiewet* (Telecommunications Act) that entered into force on 19 May 2004.[22] Other legislation transposing parts of this directive are amongst others the *Wet op de Economische Delicten* (Act on Economic Offences), that implements Article 13(4) of Directive 2002/58/EC.

Police data

The *Wet Bijzondere Opsporingsbevoegdheden* (Special Investigative Powers Act) for the investigation and prosecution of serious and organised crime entered into force on 1 February 2000. Under the act the Public Prosecution Service is assigned a number of special powers of investigation, including systematic observation, criminal civilian infiltration and bugging by means of wiretapping equipment. A key element in the legislation concerns regulations to monitor these powers of investigation. Individuals against whom these special powers of investigation have been used must be informed in accordance with the law at a certain point in time, unless they are already aware thereof following criminal proceedings.

On 13 December 2004, the Minister of Justice sent the Lower Chamber an evaluation report for the Special Investigative Powers Act, confirming that the duty to inform (referred to as the duty to notify) is observed to a very limited extent only *(see WODC report 'The Special Investigative Powers Act: concluding evaluation, 2004, www.wodc.nl)*. Reasons given include the fact that notification is not required until such is permitted in light of the investigation, the fact that failure to notify is not penalised and the fact that the obligation to notify is not a priority for the public prosecution. In his accompanying letter of 13 December 2004 the Minister of Justice announced measures to promote compliance.

The special investigative powers constitute a radical violation of individuals' personal lives through the secretive gathering of data and placing wiretapping equipment in a private environment. When the special investigative powers were introduced, one of the guarantees which the legislators evidently deemed necessary to protect individuals' personal lives and personal data was not considered a priority for years with the public prosecution. According to the Dutch DPA this presents an alarming image of disregard of privacy guarantees.

A Bill on the processing of police records was submitted to the Lower Chamber on 17 October 2005. This act entails a radical review of the Police Files Act *(Wet politieregisters)* as it exists today. Key aspects of Dutch DPA's comments on the preliminary draft were not dealt with: data are not assigned a code indicating the reliability (the difference between soft and hard information) and risk of failure, there are insufficient guarantees against the provision of data to third

[21] Act of 6 July 2000, concerning regulations regarding the protection of personal data (Wet bescherming persoonsgegevens), Bulletin of Acts, Orders and Decrees 2000 302. An unofficial translation of the act is available at the website of the Dutch Data Protection Authority, www.dutchDPA.nl or www.Dutch DPAweb.nl

[22] Act dated 19 October 1998, concerning regulations regarding telecommunication (Telecommunications Act), Bulletin of Acts, Orders and Decrees 2004, 189.

parties of limited reliability, and there are no additional guarantees for data on unsuspected individuals and an excessive collection of data on individuals not under suspicion

The fight against terrorism and intelligence services

The Investigation of Terrorism Increased Powers Act *(Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven)* was submitted on 17 June 2005. Under the Bill police and justice authorities may tap telecommunications and record confidential communications using wiretapping equipment, systematic observation, and infiltration if there is evidence of terrorist crimes. It also offers the opportunity to postpone perusal of court documents for long periods of time. The criterion 'indications' is less strong than the common criterion of 'suspicion' as grounds for using investigative powers.

In its Opinion of 26 May 2005 the Council of State pointed out that the Crimes of Terrorism Act *(Wet terroristische misdrijven)* which came into force on 1 September 2004 has already made punishable offences committed in the preparatory phase of terrorist crimes, which enables application of powers of investigation and means of coercion at an early stage. This new Bill provides a range of options to take precautionary steps against terrorist offences from an early stage. These options are a drastic change from the existing system of investigative powers and criminal prosecution and, according to the Council of State, demand a thorough substantiation of their need. In applying the proposed powers of investigation, there is an obligation to report (duty of notification) to the citizen, to enable the latter to use a means of recourse as referred to in Section 13 of the ECHR against violation of his fundamental freedoms. In its opinion the Council of State refers to the failure to observe the duty to notify previously introduced under the Special powers of investigation Act (Section 126bb Criminal Code). The government is advised to report how the obligation of the duty to notify is observed.

On 22 December 2004 the Dutch Data Protection Authority *(College bescherming persoonsgegevens)* submitted its Opinion on a preliminary draft of an act to broaden the investigative powers in terrorist crimes, which, based on the protection of data, took a critical look at the expansion of the powers of authority, the collection and processing of soft information and the failure to comply with the duty to notify.

Measures to combat terrorism also include the intensification of data exchanges between the Public Prosecution, the Police, the Immigration and Naturalisation Service (IND) and the General Intelligence and Security Service *(Algemene inlichtingen- en veiligheidsdienst, AIVD)* through the so-called *Contraterrorism infobox* (CT Infobox). Recognising the importance of data exchanges to combat terrorism, the Dutch Data Protection Authority urges clear descriptions of the legal basic principles, the responsibility and powers of participating parties and adequate supervision. After all, the processing of personal data within the framework of prevention of terrorist crimes may considerably increase the risk that innocent individuals who are included in databases based on certain characteristics or alerts are not treated fairly by the government or society.

Market operation in healthcare

Over the past few years, a radical change in the healthcare and healthcare insurance funding

system was prepared for the purpose of increasing cost control in healthcare. The new system is based on the idea that competition between insurance companies will favourably influence the price and quality of healthcare. The Bill for the Healthcare Insurance Act was submitted on 17 September 2004. The parliamentary debate on the bill was rounded off in 2005 and the act entered into force on 1 January 2006. Although under the new system detailed medical data per patient and treatment are provided to the insurance companies, the privacy guarantees are not laid down by law. Instead, these are laid down in a Ministerial Order and a Code of Conduct for the healthcare insurers.

In a number of Opinions, the Dutch DPA criticised the implications of the new system for the protection of personal data. Dutch DPA's main objections are:

- The broad scope of the obligation that healthcare providers have to submit patient's personal data to the healthcare insurers compromises the grave duty of medical professional secrecy and patient confidentiality. The so-called Diagnosis Treatment Combinations *(Diagnose Behandel Combinaties)*, which are the key for the data exchange between care providers and insurance companies, supply more detailed data on patients than the Diagnose Related Groups system used in other European countries;

- Failure to make arrangements for the protection of medical data in the preparation and realisation of the new system. The basis for the provision and processing of medical data and the guarantees are not arranged in the Act itself, but will be worked out in subordinate legislation and through sector arrangements. Preventing the re-use of medical data for supplementary insurance or other products and services offered by the insurance companies will depend exclusively on self-regulation schemes and the vigilance of the insured and the people applying for insurance.

Personal Public Service Number

A proposal for the Personal Public Service Number General Provisions Act *(Wet algemene bepalingen burgerservicenummer)* was submitted on 22 September 2005. The personal public service number (*burgerservicenummer*, BSN) will replace the current tax and social insurance number *(sofi-nummer)* which is issued by the Tax Office and used as registration number for tax purposes and social security. The BSN is a general and unique registration number for every citizen used for all government services. All government bodies may use the BSN to process personal data within the framework of their task without separate legal regulations being required. The BSN will also be assigned to hundreds of thousands of non-residents (EU citizens and Dutch nationals abroad) who deal with the government on a regular basis; however, plans have not yet been worked out and this will not be realised when the BSN is introduced. The trade and industry sector has asked to be permitted to use the BSN. There is no clarity on this point as yet.

On 10 February 2005, the Dutch DPA published an Opinion on the preliminary draft of the Bill and concluded that it did not contain sufficient guarantees to ensure personal details were handled with due care. Without such guarantees the regulation was considered to violate Section 8, subsection seven, Directive 95/46/EC, which states: *The Member States*

adopt the conditions under which a national identification number or any other general means of identification may be used for processing purposes. This stipulation is ignored in the Bill of 22 September 2005. In its Opinion of 1 July 2005 the Council of State also concluded that the introduction of the BSN without adopting rules and mechanisms to protect personal data is irresponsible.

The Dutch DPA is of the opinion that the Bill submitted on 22 September 2005 fails significantly as regards reducing the risks associated with the introduction and use of the personal public service number. The introduction of the BSN should take place only after guarantees for its careful use have been defined and embedded in legislation. In a letter dated 25 October 2005 the Dutch DPA asked the members of the Permanent Committee for the Interior and Kingdom Relations of the Lower House to consider the interests of the individual citizen, and it responded as follows:

The argument that a citizen always benefits from an efficient government and therefore a general registration number ignores the far-reaching implications of the introduction of the personal public service number. Above all, the BSN is useful for the government, while the risks for the citizen are insufficiently recognised or contested:

- *'computer errors' can spread much quicker via the BSN*
- *there are no rules for informing citizens on substantial errors in the processing of their data*
- *the individual citizen will experience great trouble having any errors corrected and there is no specific 'desk' for any problems*
- *it is easier for governments to gather data without authorisation*
- *identity fraud will increase.*

The Dutch DPA recognises fully that a general citizen registration number has advantages in respect of creating a more responsive government and reducing administrative costs. An unambiguous identification of citizens and the reuse of basic data may also serve to protect personal data. For the citizen, the protection of his personal data and social acceptability of the introduction of the personal public service number, the Dutch DPA therefore attaches great importance to clear legal regulations concerning:

- *the conditions under which the BSN may be used*
- *the government bodies (and companies, if any) who can use the BSN*
- *that citizens are informed of mistakes and errors found*
- *the set-up of an effective ombudsman function for citizens*
- *requirements being established for the ICT security of files using the BSN.*

B. Major case law

Scope of the right of access

In 2004 a dispute between a bank and thousands of citizens over the right of access resulted in a number of court cases. When the stock markets crashed in 2000 and 2001, many thousands of holders of share lease contracts with Dexia Bank Nederland N.V. (Dexia) lost large amounts of money. Duped customers asked to see their files. Dexia did not co-operate. Granting the customer's demands could harm its position in legal procedures and lead to disproportional administrative costs.

Following mediation requests, the Dutch Data Protection Authority decided on how the right of access should be interpreted in this situation.

The Dutch DPA was of the opinion that Dexia should provide the data demanded, but Dexia ignored this decision. Decisions by the Disputes Committee for the Banking Industry *(Geschillencommissie Bankzaken)* and the court cases that followed have varied on the application of this right.

Some cases are still in the appeal court. It is not quite clear if a request for access should be motivated, which data exactly should be supplied and in which cases the processing party can invoke the grounds for exclusion set out in Article 13, Directive 95/46/EC and Section 43 WBP. Opinions held by the supervisory authority and the trade and industry conflict.

C. Major specific issues

Integrated vision on human rights: foundation of a new institute

Four organisations, the Equal Treatment Commission *(Commissie Gelijke Behandeling)*, the National Ombudsman (Nationale ombudsman), the Netherlands Institute of Human Rights *(Studie- en Informatiecentrum voor de mensenrechten)* and the Dutch Data Protection Authority submitted a proposal for the foundation of a national human rights institute to the government in September 2005. According to the authors of the proposal, the proposed institute should have a number of tasks including a desk function, providing advice, and arranging for education and research.

The organisations found that it may be necessary to approach social developments from an integrated point of view on human rights. For example, the implications of collecting, using and issuing or publishing personal data cannot always be assessed by exclusively testing them against practical guarantees for the protection of personal data. Other fundamental freedoms are equally compromised in, for example, the large-scale spreading of personal data via publications on the Internet and these include the freedom of speech, freedom of communication and the ban on discrimination. Collecting data on minority groups may serve the principle of equality **and** lead to discrimination. The policy proposals for combating terrorism touch upon various basic freedoms. The use of biotechnology and radio frequency identification (RFID) are other examples of social developments where the recording of personal data can play a large role and which touch upon various fundamental rights and freedoms such as personal dignity, the right of freedom and the principle of equality.

Survey 'Citizens and their privacy'

The Dutch DPA commissioned a survey into the familiarity amongst citizens on privacy legislation and the importance they attach to the protection of personal data. Similar surveys have already been carried out in a number of European countries.

From the survey it emerged that citizens attach great importance to the confidentiality of their data with the tax office, financial institutions, social security services, insurance companies, debt collection agencies, the police, and so on. However, they do not have absolute confidence in the notion that their data will be treated with due care.

The survey also showed that citizens have very balanced ideas about the protection of

personal data compared with other interests. The majority of citizens indicated they wanted to allow other (competing) interests, but subject to restrictions. For example, blacklisting and checking emails and use of the Internet at work is found acceptable, provided there are concrete indications that justify this alerting or monitoring.

From the survey it also emerged that just over half of all citizens know about the Data Protection Act. In view of the support that citizens voice for the protection of personal data, it may be concluded that there is undeniable support in Dutch society for legislation with the purpose of protection of personal data. When asked, an amazing 92% of all citizens respond that they attach great to very great importance to the existence of legislation in this field.

Despite the intense publicity on safety and terrorism at the time the survey was carried out, citizens clearly indicated that the protection of personal data by the government and trade and industry must be properly regulated.

Poland

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

On 12 July 2005, Poland ratified the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and cross-border data flows (published in Journal of Laws of 2006 No. 3 item 15). The Additional Protocol entered into force on 1 November 2005.

As far as the implementation of the Directive 2002/58/EC is concerned, legislative work was conducted during 2005 in connection with the amendment of the Act of 16 July 2004 – Telecommunications Act. The amendment (the Act of 29 December 2005 on the amendment of Telecommunications Act and the Code of Civil Procedure) *inter alia* provides that the operator of a public telecommunications network or the provider of publicly available telecommunications services which process traffic data concerning subscribers and end users is obliged, due to the performance by authorised bodies of national defence, security and public safety and order related tasks and duties, to store this data for two years (new wording of the Article 165 of Telecommunications Act). Another proposal submitted during the amendment work provided for the obligation to store traffic data for 15 years. However it was strongly opposed by the interested parties. The provisions impose the obligation to delete or make the data anonymous after the expiration of the prescribed term as well as provide the security and confidentiality of that data and data subjects interests with due diligence.

A draft of the Act on Disclosure of Information and Communistic Secret Service Documents covering the years 1944-1990 and the Contents of Those Documents was prepared by the deputies of the ruling party. The draft introduces amendments into the lustration provisions which have been in force so far and provides for a wider range of persons subject to the lustration including persons performing public functions, including journalists and university professors. The new draft provides for the citizens' right to control information on persons performing public functions and professions of public trust which would be exercised by giving the citizens access to files of persons who are subject to lustration. Moreover, the Institute of National Remembrance (the IPN) will issue certificates for vetted persons describing the contents of secret service files which will then be published in the IPN's register available on the Internet.

The new Article 105a has been added to the Banking Act under the Act of 15 April 2005 on the amendment of the Protection of Classified Information Act and some other acts. According to that provision banks and other institution authorised to grant credits by the act or credit information agencies may process information on individuals (consumers) for the purpose of credit worthiness assessment and credit risk analysis. These institutions may process information after the expiration of the obligation under a contract concluded with bank or other institution authorised by the act to grant credits provided that the data subject has granted his/her consent in writing. The consent in question may be revoked at any time.

The institutions may process information in such a situation if all of the following requirements are met:

1) an individual concerned did not fulfil the obligation or is in arrears with performance under the contract concluded with bank or other institution authorised to grant credits by the act by more than 60 days;

2) if the circumstances referred to in point 1 have occurred, information may be processed only after 30 days from the date of the notification of the intention to process personal information covered by the bank secrecy without the consent of the data subject is provided. Information may be processed without the consent of the data subject for no longer than five years from the date of the expiration of an obligation.

The provisions of Personal Data Protection Act of 29 August 1997 and law enforcement provisions to this Act have not been amended in 2005.

B. Major case law

Among the Judgements concerning privacy and data protection covering the reporting period, a special mention should be made of the Constitutional Tribunal's Judgement of 12 December 2005. The Tribunal stated that a discrepancy existed between the Constitution of the Republic of Poland and some provisions of the Police Act of 16 April 1990 which regulates the collection and use of materials obtained in the course of an operations audit conducted without the permission of the court or the written permission of the person sending or receiving the information. Moreover, the provision challenged does not specify the scope of information that may be collected in that way nor the situation when such a collection should not be conducted. The Tribunal stressed that the above-mentioned provision does not provide for the possibility to inform interested persons about the operations audit except at the time when audit is conducted. However, after that a person who has been investigated shall have access to his/her data that was collected. In the same Judgement the Tribunal also challenged the compliance between the Constitution of the Republic of Poland and the order by the Chief Police Commander concerning collection, processing and use of information by the police because the rules and procedures of collection and disclosure of information on citizens may be regulated only by an act. The above-mentioned provisions shall cease to be applicable within 12 months from the date of Judgement's publication.

On 26 October 2005, the Constitutional Tribunal decided on a discrepancy between the Constitution of the Republic of Poland and the provisions of the Act on the National Remembrance Institute – Commission for the Prosecution of Crimes against the Polish Nation which provide for the right of access to documents and appropriate rectification but only on the condition that one should have the status of an 'aggrieved person'. The Tribunal stressed that the constitutional right to rectification or deletion of information which is incomplete or unlawfully collected cannot be limited only to a given category, i.e. aggrieved persons. In the Tribunal's view, the Act on the IPN allows interested persons to enclose updates, documents or copies which should be accepted by the IPN and attached to appropriate files. This solution should guarantee that information gathered based on the collected documents is true, complete and objective.

In 2004-2005 the Inspector General was dealing with numerous cases concerning disclosure of debtors' personal data to debt recovery

companies under the assignment of receivable debts. The sharp practice of some debt recovery companies often comprises intimidation against consumers and charging court costs in an arbitrary way. Whereas, from the point of view of Personal Data Protection Act, the lawfulness of the processing of debtors' personal data by debt recovery companies is of the key importance here. The Inspector General presented the view that a disclosure of consumers' personal data in connection with the assignment of receivable debts may only take place with the data subject's consent. In such a situation, none of prerequisites of the lawfulness of the processing of personal data laid down in Article 23 paragraph 1 of the Act should apply. The cases concerning the processing of personal data in connection with the assignment of receivable debts were decided on both by the Voivodship Administrative Court in Warsaw and the Supreme Administrative Court. It should be clearly stressed that at present this issue raises many doubts in the case law of the administrative courts. On 6 June 2005, the Supreme Administrative Court with an enlarged panel of seven judges issued the decision that has established a precedent. The Supreme Administrative Court stated that in the case of the assignment of receivable debts, consumers' personal data may be disclosed to assignees under the Article 23 paragraph 1 point 5 of Personal Data Protection Act which says that the processing is permitted if it is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject. However, the Supreme Administrative Court stressed that the assessment of possible violation of consumers' rights and freedoms should be made on a case-by-case basis.

C. Major specific issues

At the beginning of 2005, public opinion was moved by the case of disclosure of personal data included in records of the National Remembrance Institute – Commission for the Prosecution of Crimes against the Polish Nation (the IPN), the tasks of which comprise, inter alia, storing, analysing and disclosing of files of the former communist-era secret service. A well-known journalist had posted on the Internet evidence that the IPN's archival resources available in the reading room contained about 200 000 names and surnames of individuals whose files are being stored in the IPN archives. These files covered personal data of both the secret service collaborators and the employees, as well as individuals who were wronged by the secret service, without a determination of particular categories.

Following that incident, the inspectors of the Bureau of the Inspector General for Personal Data Protection conducted an inspection of the processing of personal data by the IPN. In the course of the inspection it was found that the above-mentioned list/evidence was created for the purpose of browsing through the archival materials and was not protected against damage, change or making a copy by the readers. The inspection revealed a non-compliance with the Personal Data Protection Act inter alia in the form of numerous breaches of data security rules which should be observed in the case of processing of personal data in computer systems. It was also found that there was no list of persons authorised to process personal data. Moreover, IPN had not notified their data filing systems for registration with the Inspector General and made the data contained in its archives available to journalists despite

the fact that this is not provided for by law. The Inspector General issued a Decision which orders the remedying of the negligence concerning the processing of personal data in the IPN.

However, it has been appealed against and at present awaits settlement in the Supreme Administrative Court. The Inspector General also informed the public prosecutor's office that the offence had been committed, but the proceedings concerning that case have been discontinued by the public prosecutor's office which stated that there has been no offence committed, even though the requirements of Personal Data Protection Act have not been met.

Portugal

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The Directive 95/46/EC was incorporated into national legislation by Law 67/98 of 26 October 1998 – Data Protection Act.

The Directive 2002/58/EC was incorporated into national legislation by Decree-Law 7/2004 (only Article 13) and by Law 41/2004 of 18 August 2004.

During 2005, important legislation related to data protection issues entered into force, in particular Law 1/2005 of 10 January on the use of video surveillance by law enforcement authorities, and Law 12/2005 of 26 January on personal genetic information and health information. Both laws received the prior Opinion of the Portuguese Data Protection Authority, which made a lot of suggestions to improve the texts.

Additional legislation concerning the use of video surveillance in highways for the purpose of traffic regulation, detection of infractions and prevention of accidents was also approved in 2005.

B. Major case law

Within the possibility of appealing a DPA decision under the Data Protection Act, the DPA faced about ten appeals concerning sanctions proceedings, and none concerning administrative decisions.

Most of the cases regarded the use of video surveillance or biometric systems without the due notification procedure and the lack of the right to information. In the majority of the cases, the court upheld the sanction imposed by the DPA and in a couple of cases the sanction was lowered.

C. Major specific issues

In general, the year of 2005 was a very active period for the Portuguese DPA and included the reinforcement of human resources, work reorganisation, development of a new internal information system related to the public registry and the electronic notification system, and a new website. This restructuring was intended to find better ways of dealing with the increasing number of notifications, Opinions, investigations, requests for information, and to provide better assistance to data subjects and data controllers.

Opinions to draft laws

Under Data Protection Act, draft legislation, either at national or international level, containing data protection matters, has to be submitted to the DPA for its Opinion. As a result, in 2005, the DPA provided 44 Opinions, some of them related to legislation in preparation in EU bodies, such as the legal basis of the SIS II, the development of VIS, and the retention of traffic data. Regarding national draft laws, the DPA gave Opinions on the incorporation of the Directive on the re-use of public information; on the access of welfare services to data held by the tax office for the purpose of checking the income of people who claim for subsidised medications; on the use of video surveillance in highways; and on the creation of a blacklist for tax debtors.

Notification fees

The DPA started to collect fees for the notification procedure. For legal persons, the fees are €50 and €100, depending whether the data processing is subject or not to prior authorisation. For natural persons, the fees are €30 and €60 respectively. The fees have to be

paid prior to or when the notification form is submitted.

Public Registry and new website

The DPA published a new website with a new structure and with much more information available. It has two research tools, one on Decisions and the other on thematic information. The website also has versions in English and French and includes legislation and jurisprudence. This new website has on line, for the first time, the Public Registry, which can be consulted by data subjects and data controllers, who can check, for instance, if a specific company to which they intend to communicate data is duly registered in the DPA. The DPA has already received some positive feedback from people consulting the Public Registry. The website can be found at www.cnpd.pt

Cross-border data flows

The DPA has also eased the procedure for cross-border data flows. The DPA decided to give prior authorisations only to the international date transfers carried out under Article 26.2 of the Directive. Whenever standard contractual clauses are used or there is an adequate EC Decision, the data processing does not require prior checking. The same applies for the situations provided for by Article 26.1 of the Directive.

E-Voting

In 2005, an e-voting pilot took place for legislative elections, where two different electronic procedures were tested: e-voting in polling stations and on-line voting. The pilot was closely monitored by the DPA which had authorised the access to the electoral database. Based on the findings of the pilot scheme, and on several discussions held, the DPA issued some Guidelines concerning "The privacy of the voters in e-voting". The DPA also held a conference in the Parliament, inviting all the universities' teams coordinating the pilot, the Elections National Commission and all the deputies. It was a very fruitful discussion and an interesting initiative.

Political marketing and electronic communications

Following the incorporation into national law of the Electronic Communications Directive and the rules regulating electronic communications for marketing purposes, the DPA issued some guidance in the field of political marketing. Anytime there is an electoral process, the DPA receives many complaints from data subjects because of political propaganda. Therefore, the DPA decided to provide the political parties with the Guidelines to be followed. This issue got some press coverage and fewer complaints were received at the next election.

Whistle blowing

The Portuguese Stock Exchange Regulator made a recommendation, last November, in order for companies to put in place a communication policy on internal irregularities. The scope was not clearly defined and no allusion to data protection dispositions was made. To prevent companies eventually developing such policies with no data protection concerns, and to find out exactly what the aim was of such communication policy, the DPA held a meeting with the Regulator and it was clarified that the scope of the communication was management and accountability. It was also decided that the Regulator would alert companies to comply with data protections rules, in particular that they should notify those data processing to obtain authorisation from the DPA.

Slovakia

Slovakia became a Member State of the European Union on 1 May 2004. The Office obtained a new official name effective as of 1 May 2005 – the Office for Personal Data Protection of Slovakia (hereinafter referred to as the 'Office') by the Act No. 90/2005 Coll. which amended Act No. 428/2002 Coll. on personal data protection (hereinafter referred to as the 'PDP Act').

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Implementation of Directive 95/46/EC

The latest amendment of the PDP Act was considered to be an adequate response to the comments raised by the European Commission in the previous years. It became effective on 1 May 2005.

Despite this, the Office for Personal Data Protection of Slovakia asked the European Commission, Directorate-General Justice, Freedom and Security Data Protection Unit to review the amended PDP Act in detail. The aim was to reach maximum possible harmonisation quality of the PDP Act with the Directive 95/46/EC.

At the end of 2005, the EC Data Protection Unit provided the Office with the comments which were discussed thoroughly in February 2006 in Bratislava with an EC expert. The discussion was very fruitful, aiming to find appropriate solutions for an effective contribution to the personal data protection in Slovakia. The recommendations and new ideas from the EC will serve as a base during the next round of the PDP Act amendment process to take place soon.

Implementation of Directive 2002/58/EC

The Directive 2002/58/EC sets out the rights and obligations within the scope of data protection specifically in the area of electronic communications. The Directive was implemented by Act No. 610/2003 Coll. on Electronic Communications within the scope of the New Regulatory Package for Electronic Communications. Implementation of this Directive falls within the competence of Ministry of Transport, Posts and Telecommunications of Slovakia.

At the beginning of 2005, the European Commission sent an official Notification on the incomplete incorporation of Directive 2002/58/EC. The Notification concerned missing provisions on 'cookies' and incomplete provisions on unsolicited communication. Slovakia answered within the given time period and proposed a solution. The process of amending the Act No. 610/2003 Coll. on Electronic Communications started with the Resolution No. 663 of the Government of Slovakia dated 7 September 2005 and finished with the adoption of the Act No. 117/2006 Coll. by the Parliament of Slovakia on 2 February 2006. The missing provisions mentioned by the EC were inserted into this act. This amendment of the Act No. 610/2003 Coll. became effective on 1 April 2006.

Annotation of Other Legislative Acts and Opinions

In 2005, the Office annotated more that 100 legislative acts from the personal data protection point of view and worked out more than 690 statements.

B. Major case law

The Office was a party in three cases during 2005. One of them was on the amount of the penalty given, one intended to reverse a Decision and one was a judicial review of the executed office procedures. The two cases were not decided in favour of the Office, however they have been appealed to the court of higher instance and one is still pending.

C. Major specific issues

Privacy and transparency

Act of the Slovak National Council No. 211/2000 Coll. on Free Access to Information was amended by the Act No. 628/2005 Coll. The amendment became effective on 2 January 2006 and was extensively promoted in the media. The latest version of the Act stipulates an obligation to more transparency in the public sector regarding the economic or financial identity of its officials and employees (e.g. managers of the state or municipal authorities, deputies etc.). It sets out to make available their personal data together with the information about their salaries and remunerations. Also it sets out to publish the personal data related to the ownership to real estate transferred from the state to other subjects. It also allows for the publication of the information about the management of property owned by the state or municipalities e.g. of its sale or rent. In that context more personal data has to be made available or published than before. The aim of the amendment is allegedly to make the public sector more transparent to the Slovak citizens. However, the Office feels that the respective amendment goes far beyond the framework of the standard personal data protection rules set up by the Directives and did not solve the lack of transparency in the share out of the budgetary resources at all. These concerns resulted in written Opinions and public statements by the Office.

Fraudulent misuse of the Personal Data and Biometrics

The Office had registered cases of personal data misuse by "second pillar pension administration companies' dealers" that were widely published on the TV and in the press. Second pillar pension administration companies are defined by the Act No. 43/2004 Coll. The dealers developed contracts on behalf of the data subjects without their explicit consent (dealers are usually paid for creation of new contracts). The second pillar pension administration companies said that the contracts were valid; the data subjects affirmed the contrary. The due social insurance fee paid for pension funds is divided into equal parts for the first pillar pension fund and for the second pillar, one. About 60 complaints by the victims were submitted to the Office.

The Office is often consulted on the necessity of using some of the biometric data of data subjects for authentication/verification purposes in banking or other private sectors. The Office received notifications about many cases of misuse of personal data, about fraud, faked contracts, money stolen from credit/debit cards, etc. The use of biometric data is becoming increasingly important in order to prevent loss or damage to customers or business partners. The relevant explicit consent of data subjects to process biometric data is required by the PDP Act only if the biometric data falls under the scope of the definition of the personal data. There is no special law in Slovakia at present which would set up specific rules on collecting, processing, using or making the biometric data available.

Former state security records disclosure

At present some people are pushing to disclose more of the secret records of the activities of the repressive state organs of former Slovakian and Czechoslovakian State from the period 1939-1989. The National Memory Institute of Slovakia has recently made public the information about the liquidation of Jewish enterprises (1941-1942). This information consists of 10 112 records including the names of so-called 'Aryanisers' who received a percentage of the value of the liquidated property. The so-called Aryanisation of the Jewish enterprises in the Second World War (1939-1945) was a product of the Nazis-imposed process for the "elimination of the Jews from the economic and social life".

International co-operation

In addition to the regular international activities in the field of personal data and privacy protection due the EU membership, the Office participates in the multilateral CEE countries' conferences that are focused on topics of particular interest to the host countries. During the 7th Meeting of the Central and Eastern Europe Personal Data Protection Commissioners in Smolenice in Slovakia on 24 May 2005, a Declaration on future co-operation between Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland and Slovakia was signed. In the area of bilateral co-operation between Slovakia and the Czech Republic, the so-called "Valtice Memorandum on Co-operation between the Office for Personal Data Protection of Slovakia and the Office for Personal Data Protection of the Czech Republic" was signed on 21 March 2006 in Valtice in the South Moravian region.

In addition, the Office is participating in events with a similar or related scope, for example conferences on Human Rights, Information Society, International Strategies and Investments, Telecommunications, Spam and Cybercrime etc. and is making efforts to create or tighten ties to the private investors and non profit organisations.

Schengen evaluation mission

The Schengen Evaluation Mission visited Slovakia in February 2006 with the aim of checking the readiness of Slovakia to implement the Schengen aquis in the area of personal data protection. In Slovakia, the Mission experts focused their monitoring to the following topics: legal, institutional and organisational framework of personal data protection, process of enforcing the rights of data subjects and the ways these claims are disposed of, supervisory activities of the Office, actual status of technical security of personal data processing, personal data protection related to process of application for/obtaining of visas, international co-operation of the Office with foreign data protection authorities, and awareness of citizens in the area of personal data protection.

The Mission's Experts summarised their findings in the evaluation report. The Office in co-operation with the Ministry of Interior worked out an official position on the evaluation report findings. Subsequently the requirements defined in the evaluation report were incorporated into timetables of the national Schengen action plan. The Office anticipates that the work coming out of this report will be addressed by end of 2006 and Slovakia will fulfil requirements requested by the EC.

Public awareness

In order to increase the implementation quality of the Directive 95/46/EC, the Office informed ministers and other representatives of state administration authorities about the new provisions of the PDP Act, in particular about the interim provisions stated in Section 52 and about the respective deadlines following from the interim provisions by section 55 of the PDP Act effective as of 1 May 2005. The majority of state administration bodies afterwards answered that they were already implementing the changes into the legislative rules in their competence or stated that the acts belonging to their competence already guaranteed such an obligation. Some bodies declared their openness to implement new provisions on the basis of a direct consultation with the Office.

In 2005 and 2006, the Office organised numerous seminars and consultations about the recently amended PDP Act and the amended data processing rules and the new obligations of controllers namely for banking and leasing sector, water supply companies, Cadastre Office, telecommunications and mobile operators, etc.

The Office created a new version of its website. Furthermore, the employees of the Office independently gave many expert lectures on personal data protection.

In order to receive quantified information about the public awareness, a public survey was performed. The awareness of citizens about personal data protection rights was 25% higher than in 1999. The poll showed that, from the citizen's point of view, the most sensitive personal data was that National ID (so called Birth ID) was considered to be the most sensitive by 72% of respondents. Data on personal property and finances was considered sensitive by 40%, health state data by 40%, biometric data by 22%, mental identity (psychical state) by 21%, rap sheet data by 13%, membership in political party – political opinions by 12%, information on sexual orientation by 12%, faith/church confession by 10%, race and ethnic data by 5%, and nationality by 5%.

Notifications of the personal data protection officials appointed by the controllers/registrations of the filing systems

As a result of the latest amendment of the PDP Act in 2005 and 2006, by 12 April 2006 the Office registered 37 500 notifications of appointment of the personal data protection officials responsible for internal supervision of personal data protection as provided by the Section 19 of the PDP Act. These notifications replaced the registration of filing systems in the vast majority of cases.

In 2005, the Office issued 31 standard registration numbers based on the provisions of the Section 26 and 25 special registration numbers in accordance with the Section 27 of the PDP Act. In 2006 up until 12 April the Office had processed six standard and seven special registrations of filing systems. By 12 April 2006, the Office had received a total of 4 639 applications for registration of filling systems processing personal data.

The Office has given its consent to 28 cases of cross-border transfer of personal data to third countries under the provisions of the Section 23 (7) of the PDP Act.

Complaints

In 2005 the Office processed 187 complaints of which 134 alleged a breach of the PDP Act. The other 53 were initiated on the basis of findings and decisions of the Chief Inspector. Another 16 complaints were pending from the year 2004 and were completed in the year 2005.

Of the 150 complaints received in 2005 the Office has evaluated 43 as being substantiated, 20 partially substantiated and 87 as non-substantiated complaints. Of these, 37 were related to public sector and 112 to private sector.

In 2006, up until 12 April, the Office had received 38 complaints.

The complaints had the following content: personal data misuse by "Second pillar pension administration companies dealers" and these were investigated by the Office in co-operation with the Office for Supervision of Financial Market and the Police; illegitimate making of personal data available/public; extent and purpose of the personal data processing; illegitimate video surveillance; illegitimate personal data disclosure to third parties; and illegitimate personal data provision to third parties.

Audits

The Department of Chief Inspector executed 63 audits of the filing systems processing personal data.

Concerning the video surveillance of public areas, the Office executed 28 preventive audits at municipal police departments, hospitals, petrol stations, hypermarkets and other places.

For all inadequacies found the proper measures were taken which have to be appropriately implemented. For the cases were no violations of law was found the respective data controllers received practical recommendations for their future actions.

Priorities: Health records

The Office's main priority for 2006 is to conduct an in-depth investigation of medical data processing. The Personal Data Protection Act of Slovakia is applicable to the processing of the personal data in the healthcare sector as the general legal regulation. The Act on the Provision of Healthcare, as the special legal regulation, provides detailed specifications of the general regulations.

Final Remark

Personal Data and Privacy Protection is a complex multidisciplinary activity. It is not possible to mention all the activities and current 'hot' issues exhaustively in a few pages of text. The rapid development of new and emerging technologies and electronic services for processing personal data means that adequate legal protection is always falling a few steps behind. All these new technologies, applications and systems have to be uncompromisingly evaluated from the data protection perspective.

We especially welcome the international co-operation within the Article 29 Working Party which will help us reach the highest possible quality of personal data protection in our country.

Slovenia

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The new Personal Data Protection Act was adopted on 15 July 2004[23] by the National Assembly of the Republic of Slovenia. It entered into force on 1 January 2005. The main purpose of the new Personal Data Protection Act of the Republic of Slovenia was harmonisation with provisions of Directive 95/46/EC.

According to the new Act the National Supervisory Body for Personal Data Protection was to begin to operate on 1 January 2006.

On 30 November 2005 the National Assembly of the Republic of Slovenia adopted the Information Commissioner Act[24] which entered into force on 31 December 2005. With this Act a new state body, i.e. the Information Commissioner, was established and his duties and powers ware defined.

The Inspectorate for the protection of personal data performed all tasks and competencies of the supervisory body as required by the new Act independently from the Ministry of Justice in the period from 1 January 2005 to 30 December 2005.

The Information Commissioner is an autonomous and independent state body, competent for:

- deciding on the appeal against the Decision with which a body refused or dismissed the applicant's request for access or violated the right to access or re-use of public information in some other way, and within the frame of appellate proceedings also for supervision over implementation of the Act regulating the access to public information and regulations adopted thereunder;
- inspection and supervision over the implementation of the Act and other regulations, governing protection or processing of personal data or the transfer of personal data from Slovenia, as well as carrying out other duties defined by these regulations;
- deciding on the appeal of an individual when the data controller refuses his request for data, extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the Act governing personal data protection;
- filing a request to the Constitutional Court of the Republic of Slovenia to assess the constitutionality of statutes, other regulations and general acts issued to exercise public powers if the question of constitutionality and lawfulness arises in connection with a procedure it conducts (in cases reading access to public information and personal data protection).

The Information Commissioner is also a violations body, competent for supervision over the Information Commissioner Act and the Personal Data Protection Act.

The Information Commissioner started work on 31 December 2006 when it assumed the tasks, competences and employees of the former Commissioner for Access to Public Information and the former Inspectorate for Protection of Personal data.

With the adoption of the Information Commissioner Act and the establishment of the Information Commissioner, Directive 95/46/EC was fully incorporated into the Slovenian legal code.

Directive 2002/58/EC was incorporated into the Slovenian legal code by the Electronic Communications Act[25] which was adopted on

[23] Official Gazette of the RS, No. 86/2004
[24] Official Gazette of the RS, No. 113/2005
[25] Official Gazette of the RS, Nos. 43/2004 and 86/2004

9 April 2004 and which entered into force on 1 May 2004. Chapter X of this Act mostly regulates the protection of personal data, privacy and confidentiality in electronic communications

B. Major case law

In 2005, the Inspectorate for the Protection of Personal Data (hereinafter referred to as the Inspectorate) issued five Decisions by which it allowed private and public sector persons a limited execution of biometric measures over their employees. The Decisions were issued to four banks, which were allowed to execute biometric measures over employees having access to Treasury and Treasury adjacent areas as well as areas where computer equipment for personal data processing is installed. A mobile telecommunications company was also allowed limited execution of biometric measures over employees having access to the company's systems areas (switchboards, server rooms, computer centres).

The Inspectorate also issued a Decision establishing that execution of biometric measures over all employees merely for the reasons of recording absence or presence at work is in violation with the provisions of the law. It has been established that recording of presence and absence from work is not of vital importance to the performance of the company's activities, and the execution of biometric measures would therefore represent a disproportionate and unnecessary intrusion into the employee's privacy, as recording of presence at work can also be achieved with less invasive methods.

In August 2005, the Inspectorate issued a Decision to prohibit disclosure of data revealing the information that listed business companies in which a person identifiable by name and/or surname is elected as a representative, management member, founder or a member of supervisory board. The Decision was issued to a company offering such information to its clients over the Internet against payment. When entering the name and/or surname of a natural person into the company's search engine software, the user would receive a printout of all business companies in which the person in question appeared as a representative, management member, founder or a member of supervisory board. The company acquired this information from the Slovenian business register and other publicly accessible sources. The Inspectorate's standpoint on the matter was that the company established a new and illegal personal data filing system. The company also illegally revealed or transmitted to its clients, the information revealing in which commercial companies a certain person appears as a representative, management member, founder or a member of the supervisory board, the company at the same time altered the purpose for which this personal data was initially collected in the public registers. The company filed a lawsuit against the Inspectorate's Decision, which the Administrative Court dismissed on grounds that the Inspectorate's Decision should first be appealed to the Ministry of Justice as the Inspectorate in this transitional period (until the establishment of an independent and autonomous supervisory body) still served as a body subordinated to the Ministry of Justice. The Administrative Court's decision was appealed to the Supreme Court which ruled that the Ministry of Justice no longer had competency to decide on appeals against the Decisions of the Inspectorate, which in turn means that the Inspectorate's Decisions from 1 January 2005 onwards can only be challenged with a lawsuit at the Administrative Court of the Republic of Slovenia.

The Administrative Court refused a lawsuit against the Inspectorate in November 2005 in relation to video surveillance in an apartment building. It upheld the Inspectorate's Decision, stating that, while the execution of video surveillance of entries and exits into apartment buildings and common areas, when agreed on by the majority of co-owners, provided that a suitable protection of video footage is in place, is in fact allowed, it is however not permitted to enable real-time or taped airing of footage of the video surveillance systems via internal cable television. The airing of video surveillance footage via the internal cable television represents a disproportionate and excessive intrusion into an individual's privacy, and in addition such an airing also fails to assure the protection of personal data from access by unauthorised persons.

In 2005, the Constitutional Court decided that the Act on Referendum and Public Initiative is unconstitutional in one part, since personal data including signatures that were collected for purposes of providing the support for the initiative for referendum are a part of the materials in any further referendum proceedings. It should either be decided by the legislator that they should not be a part of these materials or their protection should be guaranteed in some other manner. Such regulation was contrary to Article 38 of the Constitution.

In another case in 2005, the Constitutional Court decided that the provisions of the Commercial Companies Act are not unconstitutional, since they allow for obligatory publication of certain personal data of sole traders (independent entrepreneurs), which are also natural persons, in their annual reports that are available to the public without limitation. This 'publicity' provision is acceptable from the viewpoint of the Constitutional Court since it relates to entering into legal contract with business subjects. The test of proportionality was applied by the Constitutional Court.

In 2005, the Constitutional Court annulled the first and second paragraphs of Article 29 of the Payment Transactions Act, in the part which addresses natural persons who are not private persons. The abrogated paragraphs stated that the Register of Accounts controlled by the Bank of Slovenia contains information on the transaction account holders (for natural persons name and surname, address, account number, title and the identification number of the bank handling the transaction account and information on whether the account balance is negative) and that information on transaction accounts are public and accessible on the Bank of Slovenia's internet pages. The Constitutional Court ruled that the Act was unconstitutional as it failed to specify the purpose of the use of the information, and in addition even enabled the collected data to be used for unspecified purposes, which is a violation of Article 38 of the Constitution per se. In relation to the Decision of the Constitutional Court it also needs to be mentioned that the Inspectorate prohibited the Bank of Slovenia from publishing data on transaction account holders which are not private persons, immediately after the entry into force of the challenged provisions.

C. Major specific issues

The Personal Data Protection Act which entered into force on 1 January 2005 specifies in considerable detail the conditions under which the video surveillance of entrances to business premises, apartment buildings and working areas can be allowed. In accordance with these provisions the persons executing video

surveillance do not need to obtain permission from the Supervisory body to establish video surveillance. The persons executing video surveillance are only required to align their implementation of video surveillance with the provisions of the law, that is, to adopt a decision on video surveillance execution, publish an appropriate notice, inform its employees in writing, obtain the consent of apartment buildings co-owners, consult the syndicates, etc. However, most of the video surveillance controllers failed to adjust their practice to be within the provisions of the law which led to a large number of appeals filed with the Inspectorate.

The new Personal Data Protection Act also prescribed conditions under which biometric measures are allowed. These measures can, if not stipulated in a specific act, be performed only in cases when absolutely necessary to carry out a business activity, for safety of people and property, or to protect confidential data and business secrets. In such cases the controllers of biometric measures must provide the Inspectorate with a prior description of the biometric measures planned and the reasons for their introduction. The use of biometric measures is allowed only after the receipt of the Inspectorate's decision allowing the use of biometric measures. A problem arose with this as the law failed to stipulate the course of action for those controllers using biometric measures prior to the adoption of the new law. With regard to this matter the Information Commissioner argued that such controllers are obliged to provide the Inspectorate with a description of the biometric measures and the reasons for their introduction, and are only allowed to continue using them after the receipt of the Inspectorate's Decision granting their use.

Several inconsistencies were also caused by provisions relating to contractual processing of personal data. Experience showed that contracts concluded between personal data controllers and contractual processors are often inadequate as they lack a specific definition of the contractual processor's competencies. These contracts also inadequately specify procedures and measures to protect personal data when in the hands of the contractual processor.

One of the persisting key problems in the area of personal data can also be discerned from the fact that most of the personal data controllers have yet to notify the supervisory body with a description of their personal data filing systems and enter them into the register of filing systems managed by the supervisory body. The register of filing systems is published on the Information Commissioner's web page and allows everyone to review in a simple manner information on filing systems' controllers in the Republic of Slovenia, information on filing systems managed by the individual controllers, types of personal data contained in individual filing systems, the purpose of processing, etc.

According to new Personal Data Protection Act the supervisory body for the protection of personal data obtained an express authority to carry out preventive measures. In accordance with these authorities the Inspectorate prepares and publishes Opinions, explanations and instructions in relation with processing of personal data in individual fields, however, due to the lack of personnel employed, the Inspectorate was unable to carry out its responsibilities to their full extent in 2005.

In 2006, the Information Commissioner plans to employ seven additional specialists in the field of personal data protection.

Spain

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Directive 95/46/EC of the European Parliament and Council of 24 October 1995 was incorporated into Spanish legislation in Organic Law 15/1999 on the Protection of Personal Data.

Link: https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf (Spanish)

The text of the Law may be viewed in English through the following link: https://www.agpd.es/upload/Ley Orgánica 15-99_ingles.pdf

Throughout 2005, progress continued in the preparation of General Regulations stemming from the Law and the new Agency Statutes which replace those approved by Royal Decree 428/1993, as a result of the application of the LOPD and the powers vested in it by the General Telecommunications Law. It is important to highlight the total transparency with which the AEPD has undertaken this work, allowing all interested sectors and citizens to submit their proposals and opinions. The Regulations are currently in the formal review stage at the Ministry of Justice.

In addition to the development of regulations arising from the Organic Data Protection Law, the legal framework this law provides has been supplemented by various general or sector rules at different levels of application which comprise the body of legal rules applicable to data protection. Amongst such rules and, specifically with reference to those published in 2005, the following must be highlighted:

Royal Decree 1553/2005, of 23 December, which governs the issuance of national identity cards and digital signature certificates.

This Royal Decree was issued after a prior compulsory report from the Spanish Data Protection Agency, and its text includes express references to Organic Law 15/1999, of 13 December on Protection of Personal Data. Furthermore, and prior to the study of the articles comprising this regulation, the Agency participated actively in the development of the project for the implementation of the DNI Electrónico (Electronic National Identity Card) as a member of the Coordination Committee set up for this purpose by Resolution of the Council of Ministers of 23 December 2004. The Agency was also an active member of the Technical Support Committee that worked on this issue and the Working Groups established for validation and orientation in the development of the relevant regulations.

Organic Law 1/2005, of 20 May, authorising Spain's ratification of the Treaty establishing a Constitution for Europe, signed in Rome on 29 October 2004.

Royal Legislative Decree 2/2004, of 5 March, which approved the revised text of the Law Governing Local Treasury Departments.

Regional Government Regulations:

Decree 309/2005, of 18 October, which approves the Statutes of the Basque Data Protection Agency.

Directive 2002/58/EC of the European Parliament and Council of 12 July, concerning personal data processing and the protection of privacy in

the electronic communications sector, which repealed the General Telecommunications Law 32/2003 of 3 November. This Law is developed in Royal Decree 424/2005, of 15 April, which regulates the conditions necessary for the provision of electronic communications services, universal service and user protection.

B. Major case law

During 2005, a total of 99 Judgments were issued by the *Audiencia Nacional* (Spanish National High Court), with appeals filed in courts of first and last instance, 12 Judgments were issued by the Supreme Court resolving appeals for reversal or reversals for doctrinal coherence and one Record of an appeal for reversal was ruled inadmissible. This report will refer only to those Judgments in which precedents were established in controversial issues and aspects of data protection that involve complex interpretation.

Communication of data to the Court in dismissal proceedings

The Judgment of 19 October 2005 dismissed the appeal filed against the Agency resolution to suspend actions undertaken in a complaint filed against the use of the plaintiff's data without consent and the communication of such data to the Courts. The use of the plaintiff's data by the defendant company did not contravene the provisions of the Data Protection regulations, as the investigatory actions taken by the company affected the maintenance and fulfilment of the labour relationship and the communications made. (Article 11.2 of the LOPD).

Processing of medical records on third parties to be indemnified pursuant to civil liability insurance

The Judgment of 21 September 2005 confirmed the Agency resolution that exonerated an insurance company and a diagnostic medical centre respectively from liability, ruling that their actions were not in violation of Article 7.3 of the LOPD. Pursuant to regulations in the sector, insurance companies must meet substantive and formal obligations that pre-suppose or require the processing of the personal data of the injured, and therefore, the co-defendant companies were exonerated from the charge of processing the plaintiff's personal data without the data subject's consent.

Communication of the insured party's personal data by the reinsurance company

The Judgment of 20 May 2005 confirmed the Agency resolution imposing disciplinary action on a reinsurance company for violation of Article 11 of the LOPD, and on a second company that assesses health status, pursuant to Article 6 of the same Law. An appeal was filed by the reinsurance company alleging that, on the one hand, it is charged with data processing for the insurance entity and, on the other, that there was no illicit communication of data to the company assessing the insured party's health status, as this is deemed to be a provision of services to the reinsurance company, both of which are envisaged in Article 12 of the LOPD. The Court examined the allegations and deemed that the documents submitted did not formally accredit the alleged legal relationship. Accordingly, it ruled that such action comprised communication of data not envisaged as permissible by Law.

Non-fulfilment of the duty to inform and the registration of data in files that do not meet the requisite security standards

The Judgement of 27 April 2005 dismissed the appeal filed against the Agency resolution on violation of Articles 5 and 9 of the LOPD. The information requirement is an inherent part of the fundamental right to data protection recognised by the Constitution, and therefore verbal information is ruled as insufficient. Thus, the Court requires a written record of such information, which the plaintiff could not furnish. With respect to security measures, the obligations set out in the Regulations on Security Measures (Royal Decree 994/1999, of 11 June) were not fulfilled, as neither the incident log referred to in Article 10 of such Regulations nor the carrier log established in Article 20 of the same had been implemented.

Communication and processing of data in contracts for the transfer of banking business

The Judgement of 16 February 2005 confirmed the Agency resolution and dismissed the appeal filed for violation of Articles 11.1 and 6.1 of the LOPD. The Court, while not questioning the commercial legitimacy of the bank business transfer, shares the view put forward by the Agency with respect to the specific transfer in question and deemed that under the LOPD this constitutes a communication of personal data comprising, in this case, the individual bank accounts transferred from one entity to another by virtue of such transaction. Moreover, if the data recipient has not verified the unequivocal consent of the data subjects, this constitutes a violation of Article 6.1 of the Law, given that the recipient of such communication is under obligation to fulfil the provisions of Article 11.5 of such Law as soon as the communication has been made.

Third party processing and compulsory guarantees

The Judgment of 9 February 2005 confirmed the Agency resolution which imposed disciplinary actions for violation of Article 6.1 of the LOPD. The existence of a contract between the plaintiff and, in this case, a state-owned University, consisting of the provision of a particular service, falls within the framework established in Article 12 of the LOPD, provided that such a contract contains the guarantees set out in such Law. As the contract does not expressly establish the security measures implemented by the data controller, the indication that the data may only be processed according to instructions from the controller, nor any commitment that the data communicated will not be used for purposes other than those set out in the said contract nor communicated to third parties, the Court ruled that the defendant committed the violation for which the disciplinary action was taken.

Sale of a CD-ROM that enables the reverse search of data

The Judgment of 26 January 2005 confirmed the disciplinary action taken by the Agency for violation of Article 11of the LOPD. The Court ruled that, in application of the regulations on telecommunications, the purpose of telephone directories, for which subscribers give their consent to be listed, is to facilitate discovering the subscribers' telephone numbers from their names and surnames. The use of their personal data is restricted to this specific purpose, which is the purpose envisaged when the subscribers consented to listing in such directories. However,

this is not the purpose behind the product which, amongst other functions, enables the user to obtain an address from a telephone number. As the data subjects in question did not give their consent for this purpose, the Court deemed that such conduct constitutes a case of illicit communication of personal data.

C. Major specific issues

Transparency: Activities undertaken to spread data protection information

One of the key priorities of the current management of the AEPD is to attain maximum diffusion of the fundamental right to data protection. Accordingly, in 2005, the Agency focused its efforts on this goal, through the participation of its Director and other members of the Agency in a broad range of activities. Such activities were addressed to public and private entities, and dealt with both general aspects of the subject and issues specific to certain sectors. The Agency participated in courses, lectures, seminars, conferences and congresses in collaboration with a diversity of institutions, which included Professional Associations, Universities, Official Chambers of Commerce and the Public Administration.

Amongst these activities, special mention must be made of the various events and courses organised, to spread knowledge of the work done throughout the year in relation to the legislative development of the Data Protection Law. In addition to the aforementioned activities, numerous meetings were held with the various players affected and over 150 interviews were given in the different news media.

Knowledge was also spread through activities undertaken in the Citizen Assistance Office, which responded to over 35 500 queries in 2005, made by telephone, in person, in writing or via the Agency website.

With the same goal of maximising knowledge of the subject, the Agency formalised ten Collaboration Agreements, in addition to the many others in place from previous years, with Universities, Associations, Foundations and a wide range of institutions.

Enforcement: The fight against Spam

Within its powers in the fight against SPAM, the Agency set up a new procedure to respond massive e-mailings, which provides advice on how to surf the Net safely and ideas on how to combat this international concern. Link:
https://www.agpd.es/upload/Canal_Documentacion/Lucha_contra_el_Spam/INFORMACIÓN SPAM (V. 30 mayo).pdf

Available in English:
https://212.170.242.148/upload/English_Resources/INFORMACI%D3N%20SPAM.INGL%C9S%20%28V.%2030%20mayo%29.pdf

Promoting self-regulation: Codes of Conduct

The codes of conduct referred to in Article 32 of Organic Law 15/1999 of 13 December aim to adapt the provisions of the Data Protection Law to the specific processing undertaken by those subject to such codes.

In 2005, a modification to AUTOCONTROL's Code of Conduct entitled "Code of Conduct in E-commerce and Interactive Advertising" was registered with the Agency with a view to adapting its original wording to the changes brought about by the continual emergence

of new technological phenomena, such as Spam. All the member entities declared their full commitment to creating and sustaining an integral self-regulatory system for advertising and commercial transactions with consumers via long-distance media within the framework of defending ethical professional conduct.

Activities related to the 'Red Iberoamericana de Protección de Datos' (Latin American Data Protection Network)

The year 2005 was a decisive one for the Red Iberoamericana de Protección de Datos (Latin American Data Protection Network), established in 2003 as a result of the initiative put forward by the AEPD, as this year brought about its full consolidation. This year the Network based its work on the activities carried out by the Specific Working Groups and through the Document on Network Strategy, now has an instrument that enables its optimal organisation and operation.

The 3rd Latin American Data Protection Conference established four Working Groups: 'Network Strategy', 'The Viability of Establishing Supervisory Authorities in the Latin American Countries', 'Access to Personal Information and Data Protections' and 'E-Government and Telecommunications'. The Groups met in Cartagena de Indias (Colombia) from 6-9 June 2005 and drafted the documents corresponding to each of these topics.

The Network currently has representatives from 17 of the 22 countries in the Latin American Community and continues to grow with the constant incorporation of new members.

Sweden

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

The EC Directive 95/46EC has been implemented in Sweden by the Personal Data Act – PDA – (1998:204) which came into force on 24 October 1998. The PDA is supplemented by the Personal Data Ordinance which entered into force the same day. The Act applies, as does the Directive, to automated processing as well as manual processing. However, the rules on fundamental principles and on when processing is permitted will not be applied before 1 October 2007 as regards such manual processing of personal data as was commenced before the entry into force of the PDA. Even though the Act, in principle, applies to processing of personal data in all sectors of society, there are several specific Acts and Ordinances that apply to processing of data in certain activities, either instead of or in addition to the PDA. Also in drafting these specific Acts and Ordinances, the Directive has been taken into account.

In the Eighth Annual Report, the proposal of the inquiry tasked with reviewing the Personal Data Act in order to see if a "misuse model" could be applied to the PDA was presented. The main feature of the inquiry's proposal was to exempt processing of personal data in unstructured material, such as continuous text, sound and images, etc from the great majority of handling regulations in the PDA. The handling rules would thus not be applicable to everyday processing like the production of continuous text in word processing software for example. One simple rule would apply instead; processing would not be permitted if it would involve improper intrusion on privacy. The proposal is now under further consideration within the Ministry of Justice and it is expected that the Government will present a bill containing such amendments during the first half of 2006.

The EC Directive 2002/58/EC was implemented into Swedish law by the entry into force of the Electronic Communications Act-ECA-(2003:389) on 1 July 2003. In chapter 6, the ECA provides rules on data protection in the electronic communications sector. Compliance with the data protection rules in the ECA are supervised by the National Post and Telecom Agency. Article 13 of the EC Directive regarding unsolicited e-mail has been implemented by amendments in the Marketing Practices Act (1995:450). These amendments came into force on 1 April 2004. The Marketing Practices Act falls under the supervision of the Consumer Agency.

During the last few years different inquiries have submitted a number of proposals aiming at facilitating the combating of crime (in 2005 several different proposals were submitted). These proposals deal with strengthened coercive measures as well as increased possibilities to collect and register personal data. The following proposals can serve as examples: *Proposal on enlarged use of coercive measures in connection with IT* (Ds 2005:6), *proposal on enlarged use of coercive measures to prevent serious crime* (Ds 2005:21), *proposal on secret room wire-tapping* (a memorandum from the Ministry of Justice) and *proposal on access to electronic communication in crime investigations* (SOU 2005:38). The proposals have been submitted to consultation with different authorities and organisations and in an Opinion of December 2005 the Data Inspection Board stated that it was essential for the legislator to make a comprehensive assessment considering

the accumulated effects of the proposals when deliberating what proposals to carry through.

In June 2004, proposals were made that aimed at widening the scope of using DNA in law enforcement. As of 1 January 2006, everyone who has been sentenced in Sweden to another penalty other than fines may have his DNA data registered in the DNA register. Until then it was only allowed to register "genetic fingerprints" from persons who had been sentenced for crimes where the penalty comprised more than two years' imprisonment. According to the new legislation persons who are not sentenced but who are, for good reasons, suspected for a crime including imprisonment may also have their DNA data registered, however in the so-called investigation register. Such data shall, if the person is convicted of a crime, be deleted from the investigation register and may instead be registered in the DNA register. If the crime investigation does not lead to an indictment, the data should be deleted from the register. The same applies, for instance, if the indictment is rejected.

B. Major case law

The question of publishing personal data on the Internet has once again been tried by Swedish courts of law. In this case the chairman of the board of a boarding school had, without consent, published information about an employed person on the school's website on the Internet. The information included personal data about the employee showing that the person in question had difficulties regarding co-operation and that he was on sick leave. As in the previous case the courts found that the processing fell within the scope of the Directive and that sensitive data had been processed. The case was brought to the Supreme Court and in its ruling of 26 May 2005 the Court found that the circumstances of this case were the same as in the Lindquist case (C-101/01) and thus the interpretation of the EC Court of Justice implied that the charge regarding prohibited transfer to third countries should be rejected. However, the chairman of the Board was convicted of contravention of the Personal Data Act as regards sensitive data.

In June 2004, the committee of the Data Inspection Board decided that collection and processing of students' fingerprints for the purpose of checking access to the school canteen was not adequate or relevant, regardless of the fact that consent would be obtained. It was stated that the checks could be made in a less privacy-intrusive manner. The Board's decision was appealed to the County Administrative Court that in March 2005 upheld the decision. The case was brought to the Administrative Court of Appeal that revoked the ruling of the lower court and stated that the municipality's need of an easy control system is of greater weight than the students' protection against intrusion of privacy. The Data Inspection Board in November 2005 brought the case to the Supreme Administrative Court, where it is still pending.

In the spring of 2005, the Data Inspection Board received a large number of complaints alleging that the Swedish Anti-Piracy Bureau (the Bureau) had collected and used data on a large scale, in particular concerning IP numbers, in connection with file sharing of copyrighted material on the Internet. The Board investigated the Bureau's processing of personal data and found that the data processed by the Bureau included data relating to offences within the meaning of

section 21 of the Personal Data Act (PDA) and was, therefore, in breach of the provisions of that section. According to section 21 it is prohibited for parties other than public authorities to process, *inter alia*, personal data concerning legal offences involving crime. The Bureau then applied for an exemption from the provisions of section 21 of the PDA for the purpose of processing IP numbers so that it could report to the police and institute proceedings against particularly serious copyright infringements, inform Internet service providers of subscribers' copyright infringements and take civil actions against copyright infringers. In October 2005 the Board decided to grant an exemption from the prohibition of processing data concerning offences pertaining to the processing of IP-numbers concerning persons who make copyrighted material available to others. The Board also decided that the exemption should only be applicable until further notice, but not later than 31 December 2006.

C. Major specific issues

The Data Inspection Board has continued to carry out certain supervisory activities in the form of specific or thematic projects. During 2005 three reports regarding such supervision have been published: *Increased accessibility to patient data* (2005:1), *Bonus cards and the Personal Data Act* (2005:2) and *Supervision of employees' use of the Internet and e-mail* (2005:3).

The Board has also published other printed matter such as the brochure *Personal data in research – what rules apply?* (together with the National Board of Health and Welfare and the Statistics Sweden) and the information leaflet *Infringement on the Internet? – Do like this!*

Also during 2005 the issue of biometric data has been the focus of public debate. As of 1 October 2005 new Swedish passports contain a chip where a digital version of the passport photo and the signature are stored. National ID cards have also been introduced which contain the same information in digital form. Later on it is foreseen that also fingerprints will be stored in passports and ID cards.

Another topic during 2005 which gave rise to a vivid discussion from different points of view, one of which was privacy, was the toll or tax on cars for passing in and out of Stockholm. It has been introduced for half a year as a trial. There have been concerns about privacy with regard to the surveillance cameras registering the cars' number plates.

As to self-regulation the Data Inspection Board gave opinions on two proposals for codes of conduct. One referred to the processing of personal data in school photo activities and the other one to the processing of personal data in connection with debt-collecting activities.

Following the adoption of the *Directive on the retention of data processed in connection with the provision of public electronic communication services*, the Swedish Minister for Justice announced that during the spring of 2006 an inquiry will be tasked with reviewing the national legislation in this field in order to propose – in consultation with the service providers – the amendments required.

The United Kingdom

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

Directive 95/46/EC is transposed into UK law as the Data Protection Act 1998 which came into effect on 1 March 2000.

Directive 2002/58/EC is transposed into UK law as the Privacy and Electronic Communications Regulations which came into effect on the 11 December 200.

B. Major case law

During 2005 there has been no major case law in the UK courts relevant to Directive 95/46/EC and Directive 2002/58/EC.

In October 2005 the Information Tribunal issued a decision in a case brought by the Information Commissioner against West Yorkshire, South Yorkshire and North Wales police. The Information Commissioner argued that the retention on record of very old convictions for relatively minor offences breached the third and fifth Data Protection Principles, being excessive and stored for longer than necessary for its purpose. The Tribunal ruled that while the information could be held for policing purposes, within six months it must not be open to inspection other than by Chief Officers of Police.

C. Major specific issues

The Information Commissioner launched a new Regulatory Action Strategy focusing on those data controllers whose failure to comply with data protection results in serious consequences, either serious harm to one individual or less serious harm to many people. Regulatory action will be taken where personal information is at risk because obligations are deliberately or persistently ignored, examples need to be set, or issues need to be clarified. The Information Commissioner also established an audit team responsible for checking an organisation's compliance with the requirements of good practice, which undertook its first audits in 2005.

The Information Commissioner's Office began publishing a series of user-friendly guides, called Good Practice Notes. These are designed to make data protection simpler by tackling common misunderstandings and addressing frequently asked questions. Topics covered in this ongoing series included electronic mail marketing, providing account information to third parties, closed circuit television and disclosing information about tenants. The Office also published a consolidated and revised version of its Employment Practices Code to help employers understand and comply with the Data Protection Act. The Code highlights the issues employers must be aware of and includes recommendations to ensure compliance. It covers four principal areas: recruitment and selection, employment records, monitoring at work and medical information. A summary guide was also developed to meet the concerns of small businesses.

The Information Commissioner issued his first authorisation of the transfer of personal data outside of the EEA using binding corporate rules. The authorisation was granted to the General Electric Company for transfers from the UK of employee data within the GE group of companies.

The Information Commissioner attended meetings with Department of Health officials

responsible for the electronic care record project, Connecting for Health, and advised on specific issues. The Information Commissioner has also taken part in workshops aimed at informing policy in this area and at improving knowledge of the eventual system for our casework teams. Connecting for Health is going through a phased implementation and plans continue to develop with active involvement from the Information Commissioner.

The Information Commissioner discussed with Ofcom the issue of Radio Frequency Identification tags prior to the regulator's consultation on whether to exempt RFID tags from radio spectrum licensing requirements. The Information Commissioner noted that in many circumstances of RFID use there will be no personal information involved and the Data Protection Act 1998 will not apply at all. In those cases where personal information is involved, it should be perfectly possible to comply with the Act.

The Information Commissioner continued to raise concerns about the proposals for an identity card in the UK, in particular that the measures in relation to the underlying National Identity Register and data trail of identity checks on individuals risk an unnecessary and disproportionate intrusion into individuals' privacy. Dialogue between the Information Commissioner and the Home Office about the identity cards proposal continued throughout 2005.

In November the Information Commissioner hosted an international conference to celebrate the 21st anniversary of the UK Data Protection Act, and to look ahead to the next 21 years. The conference also marked the retirement of Francis Aldhouse, Deputy Commissioner since the Information Commissioner's Office was established in 1984.

During 2005, the Information Commissioner provided evidence to the following Parliamentary select committees:

- European Union Select Committee inquiry into the proposed Regulation establishing a European Union Agency for Fundamental Rights
- Education and Skills Committee inquiry into Every Child Matters
- Joint inquiry of Constitutional Affairs Committee and the Office of the Deputy Prime Minister: Housing, Planning, Local Government and the Regions Committee into Electoral Registration.

During 2005, the Information Commissioner provided responses to the following consultations:

- Joint Inspections of Children's Services and Inspection of Social Work Services (Scotland) Bill, October 2005
- Northern Ireland Office's consultation paper, "Safer Recruitment in Northern Ireland"
- Improving Mental Health Information Programme consultation paper, "A Mental Health Information Strategy for Scotland"
- Department for Education and Skills' consultation on "Cross-government Guidance: Sharing Information on Children and Young People"
- Joint Money Laundering Steering Group consultation, "Prevention of money laundering/Combating the financing of terrorism: Guidance for the UK Financial Sector".

Chapter Three

European Union and Community Activities

3.1. EUROPEAN COMMISSION

The European Commission, on 16 February 2005, decided to transfer the responsibility of the Data Protection unit from the Directorate General Internal Market (DG MARKT) to the Directorate General Justice, Freedom and Security (DG JLS) in order to enhance the visibility and the coherence of the Commission's activities in this field. With this transfer the Data Protection unit will ensure the coordination and coherence of Commission's activities in the area of freedom, security and justice, in safeguarding the fundamental rights of citizens, especially the right to the protection of personal data. This decision took effect on 15 March 2005.

3.1.1. Decisions

Canada PNR Decision

Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency.

The Commission adopted an Adequacy Decision on 6 September 2006, stating that the Canada Border Services Agency is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning flights bound for Canada in accordance with the Commitments set out in the Annex to the Commission Decision. The Decision will enter into force after notification to Member States.

The Decision forms part of a package, consisting of a Council Decision on an agreement with Canada on the transfer of PNR data to the Canada Border Services Agency and Commitments from the Canada Border Services Agency on how to handle the data. These Commitments have been incorporated into Canadian law.

Joint Review PNR/USA

The Undertakings, annexed to the Commission Decision on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the US Bureau of Customs and Border Protection (CBP), provide for a joint review by CBP and the Commission on the implementation of the Undertakings with a view to mutually contributing to the effective operation of the process described in the Undertakings.

A first review took place on 20 and 21 September in Washington. The Commission was assisted by representatives from Member States' data protection and law enforcement authorities. The review consisted of a questionnaire based on the Undertakings, setting out in detail questions to be asked and issues to be raised with the CBP in relation to each Undertaking; field visits to CBP operations allowing the EU Joint Review team real-time access to live PNR data; a whole-day meeting between the CBP, the EU Joint Review team and the Department of Homeland Security's Privacy Office, aimed at discussing in detail the measures taken and the procedures put in place to oversee and manage the Undertakings.

The EU Joint Review team found that, as of the date of the Joint Review (20 and 21 September 2005), the CBP is in substantial compliance with the conditions set out in the

Undertakings. The EU team also found that it took some time before compliance was achieved, and that the CBP had received substantial assistance to achieve compliance from the DHS Privacy Office. A public version of the report can be found on the DG JLS website.

Safe Harbor / Safe Harbor Seminar

On 7 December 2005, a seminar jointly organised by the Working Party 29 and the US Department of Commerce was held in Washington. The purpose of the seminar was to confirm the WP 29 and DoC support for the Safe Harbor (SH) in order to encourage US organisations to subscribe to it, as well as to address problems related to the Safe Harbor implementation, which were identified in the 2004 Commission's Staff Working Paper on the Safe Harbor implementation (2004 Commission's report). The seminar provided an excellent opportunity to discuss data protection issues related to the SH and to other international data transfers with US organisations and US authorities. It showed the interest of companies on the question of international data transfers and in particular the growing interest of US organisations on the Safe Harbor as a mechanism to enable transfers of personal data from the EU to US as the number of organisations adhering the Safe Harbor illustrate. The seminar also provided the Commission and WP 29 with a useful opportunity to exchange views on the outstanding issues regarding the implementation of the SH with US organisations competent for enforcing the Safe Harbor (FTC and US DoC). Most participants and the US authorities deemed useful the organisation of a new seminar in Brussels in 2006 to discuss international data transfer issues.

3.1.2. Legislative Proposals

Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market[26]

This proposal presented by the Commission on 1 December 2005 aims at establishing a harmonised legal framework for an integrated payments market in the EU which will make easier cross border payments in the EU. The proposal provides that Member States shall permit the processing of personal data by payment systems and payment service providers, when this is necessary to safeguard the prevention, investigation, detection and prosecution of payment fraud. The proposal also states that this processing of personal data shall be carried out in accordance with Directive 95/46/EC.[27]

Schengen Information System II

On 31 May 2005, the Commission presented a package of legislative measures on the establishment of the second generation of the Schengen Information System (SIS II). The legislative package will replace current provisions on SIS in the Schengen Convention (Arts. 92-119).

The SIS is a common information system allowing co-operation between competent authorities in the Member States, through the exchange of information for the implementation of various policies, in order to establish an area without internal border controls. These authorities, through an automatic query procedure, obtain information related to alerts on persons and objects, which is used, in particular, for police and judicial co-operation in criminal matters, as

[26] COM(2005)603 final, 1.12.2005

[27] Art. 71 of the Proposal

well as for the control of persons at the external borders or on national territories and for the issuance of visas and residence permits.

The three proposals are a development of the Schengen aquis[28] which was integrated into the EU framework on 1 May 1999 by a protocol annexed to the Amsterdam Treaty. Although the proposals are based on different provisions of the EU Treaty or the EC Treaty, and follow different legislative procedures (co-decision and consultation to the European Parliament) they form an inseparable package as the SIS II is one single information system and operates as such. The Commission has pointed out that in order to ensure that the system is in place in 2007, the proposals need to be adopted by mid 2006.

The purpose of this package is updating the current system in order to allow the new Member States to fully apply the Schengen aquis from 2007 and lift their internal border controls. At the same time new functionalities are added to the system (for example, processing of biometric indicators, access shall be granted to Europol and Eurojust, new provisions relating to interlinking of alerts).

The legislative proposals contain provisions on data protection which take account of the regime existing in the EU in this respect. Thus, those matters falling under the First pillar shall be subject to Directive 95/46/EEC. The Data Protection Authorities (DPA) designated under Article 28(1) of Directive 95/46/EEC shall be the competent authorities to monitor the lawfulness of the processing of SIS II data in their territory. Regulation 45/2001 shall apply to the activities performed by the Commission as responsible for the operational management and functioning of the system. The European Data Protection Supervisor (EDPS) shall monitor this process. The proposal also provides that both national DPA and the EDPS shall co-operate actively.

With respect to those aspects falling under the scope of Title VI of the EU Treaty (third pillar), the protection of personal data by Member States shall be carried out in accordance with the Council of Europe Convention 108 and national independent authorities shall monitor the lawfulness of this process within their territory. With respect of processing of data carried out by Europol and Eurojust, the Europol JSB and the Eurojust JSB shall ensure the lawfulness of the activities performed by these bodies. Regulation 45/2001 shall apply to the activities performed by the Commission as responsible for the operational management and functioning of the system. The EDPS shall monitor this process. The proposal also provides that both national DPA and the EDPS shall co-operate actively.

Visa Information System (VIS)

In order to implement the Decision 2004/512/EC establishing the Visa Information System[29], the Commission had presented on 28 December 2004 a 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.[30] The proposal set ups a database on Schengen short-stay visas and provisions on the exchange of information between Member States in this regard. It contains provisions on the data that can be processed (e.g. biometrics), conditions for the exchange of information as well as rules on the protection of personal data processed in the VIS.

[28] The Convention implementing the Schengen Agreements and further provisions, mainly Decisions of the Executive Committee, implementing this Convention (and subsequent EU instruments adopted after the integration of the Schengen aquis into the framework of the European Union).

[29] OJ L 213, 15.6.2004, p. 5

[30] COM (2004) 835, 28.12.2004

Visa Information System access decision (VIS access decision)

The Council during its meeting on 7 March 2005 had asked the Commission that "in order to achieve fully the aim of improving internal security and the fight against terrorism", Member State authorities responsible for internal security should be guaranteed access to VIS, "in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats, subject to strict compliance with the rules governing the protection of personal data".

As a result, the Commission adopted on 24 November 2005 a 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.[31] In trying to meet the concerns voiced by the Article 29 Working Party[32] over VIS access by authorities other than visa authorities, the proposal limits the right of access to the VIS for purposes of the prevention, detection and investigation of terrorist offences and serious crime, via central national points on a case-by-case basis only, thereby explicitly excluding routine access. As for the rules on the protection of personal data, the future Council Framework Decision on the protection of personal data processed in the course of activities of police and judicial co-operation in criminal matters (for the Commission proposal, see below) and the Europol Convention shall apply to the processing of personal data pursuant to the Decision. Effective supervision is foreseen through the establishment of a yearly review by the European and national Data Protection Supervisory authorities.

Data retention

On 21 September 2005, the Commission presented a 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.[33] This proposal aims at implementing several declarations of the Council on the adoption of measures combating terrorism and, in particular to provide for a first pillar legal basis, as opposed to the initiative tabled by France, Ireland, Sweden and the United Kingdom in 2004.[34]

The purpose of the Commission's proposal is to complete the harmonise obligations for providers of publicly available electronic communications services or of a public communications network to retain certain traffic data, so that they may be provided to the competent authorities of the Member States for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime. The proposal provides for a period of retention of one year from the date of the communication and six months in the case of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The current EU legislation on data protection, i.e. Directive 95/46/EC and Directive 2002/58/EC remain fully applicable to the processing of personal data retained. The data so retained shall be transmitted upon request to the competent authorities (law enforcement) without undue delay. In order to alleviate the cost of this

[31] COM (2005) 600 final, OJ 2006, C 49, p.50
[32] WP 110
[33] COM(2005) 438 final, 21.9.2005; OJ 2006, C 49, p.42
[34] 28.04.2004; Council document 8958/04; see Opinion 9/2004 (WP 99)

requirement for providers of communication services, the Commission's proposal lays down the reimbursement by Member States of demonstrated additional costs incurred by providers of communication services. The proposal also amends Article 15 (1) of Directive 2005/58/EC.

Commission Communication on interoperability among European databases in the area of Justice and Home Affairs

On 24 November 2005, the Commission presented a Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs.[35] The document highlights how, beyond their present purposes, existing systems can more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime. The communication also looks into the possibility of taking other initiatives, for example the establishment of a system for monitoring entry and exit movements and a system making it easier for frequent travellers to cross external borders, or the creation of a European criminal Automated Fingerprints Identification System (AFIS). While presenting different scenarios that can be considered, the communication does not prejudge the outcome of an essential in-depth debate. It states that a delicate balance between the pursuit of these objectives and the protection of fundamental rights must be found.

Protection of personal data processed in police and judicial co-operation in criminal matters

On 4 October 2005, the Commission presented a proposal for a Council framework decision on the protection of personal data processed in police and judicial co-operation in criminal matters.[36] The Commission's intention is to guarantee the protection of personal data processed in the framework of police and judicial co-operation in criminal matters between the Member States of the EU. Wherever possible, taking into account the necessity of improving the efficiency of legitimate activities of the police, customs, judicial and other competent authorities, the proposal therefore follows existing and proven principles and definitions, notably those laid down in Directive 95/46/EC or relating to the exchange of information by Europol, Eurojust, or processed via the Customs Information System or other comparable instruments, such as Council of Europe Convention 108.

Framework Decision on principle of availability

The Proposal for a Council framework decision on the exchange of information under the principle of availability[37] was adopted by the Commission on 12 October 2005. Under the terms of this proposal, certain types of information available to the competent authorities of a Member State controlling it are to be provided also to equivalent competent authorities of other Member States and Europol. To this end, there is an obligation to notify the information that is available online through the Internet and which authorities have access to the information and for what purposes, with a further obligation to provide for consultation of index data referring to information that is not accessible online. Information which cannot be accessed online, or for which such access is not authorised, may be obtained in response to an information demand issued by a competent authority which has matched solicited information with index data, unless one of the grounds for refusal laid

[35] COM (2005) 597 final, 24.11.2005
[36] COM(2005) 475 final; OJ 2006 C 49, p. 44
[37] COM(2005) 490 final; OJ 2006 C 49, p. 45

down in the framework decision exists. Included are DNA-profiles, fingerprints, ballistics, vehicle registration information, telephone numbers and other communication data, and names contained in civil registers. For data protection it relies entirely on the future Framework Decision on third pillar data protection (see above).

Standards for security features and biometrics in EU citizens' passports

On the basis of Article 2 of Council Regulation (EC) No. 2252/2004, the European Commission adopted on 28 February 2005 a Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.[38] The Decision is addressed to Schengen Member States only. The Council had adopted Regulation (EC) No. 2252/2004 on standards for security features and biometrics in travel documents issued by Member States on 13 December 2004. This Regulation envisages the digital facial image as a first biometric feature in a mandatory manner and fingerprints as a second biometric feature also in a mandatory way. This Regulation had entered into force on 18 January 2005.

3.2. EUROPEAN DATA PROTECTION SUPERVISOR

Introduction

The European Data Protection Supervisor (EDPS) is an independent authority that primarily deals with supervision of personal data processing by the European Community's institutions and bodies. It also gives advice on proposals for legislation relating to the processing of personal data, and co-operates with data protection authorities in the Member States, as well as in the third pillar of the European Union (police and judicial co-operation in criminal matters), to ensure consistent data protection. These three tasks of the EDPS – supervision, advice and co-operation – as well his powers are laid down in Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000, further to Article 286 of the EC Treaty.

While 2004 was the first year of activity, during which a new institution was built up, the main emphasis in 2005 was on the consolidation of the EDPS in the institutional framework of the EU.

Supervision

The supervisory role is to monitor and ensure that Community institutions and bodies comply with their data protection obligations, which were laid down in 2001. There is an urgent need to develop a data protection culture and the EDPS has allowed for a transitional learning period – until spring 2007 – after which enforcement activities of the obligations will be initiated, where necessary. The major features of 2005 were:

- Further development of the network of **Data Protection Officers** (DPOs) of institutions and bodies. Independently ensuring the internal application of Regulation 45/2001, DPOs are a strategic partner in the system of supervision and the EDPS has presented a paper on their tasks. Focusing on the need for all bodies to appoint a DPO, the paper stresses that DPOs must be notified more adequately of personal data processing within their entity and that they pass on notifications of risky processing operations to the EDPS for prior checking.
- Some 34 **prior check opinions** were issued on risky processing systems (30 of which

[38] C(2005) 409 final; available online: http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm

concerned existing systems – launched before the EDPS started its activities or before the Regulation entered into effect). The following thematic priorities were identified: medical files, staff appraisal, disciplinary procedures, social services and e-monitoring.

- Twenty-seven **complaints** were received, although only five of them were declared admissible and further examined due to the fact that a large majority of complaints received fall outside the EDPS's area of competence.
- A paper was presented on how the two fundamental rights of **public access to documents** and **data protection** relate in the context of the EU administration. Work on another paper, concerning the use of **electronic communications** has begun; the paper will be published by mid-2006.
- Activities relating to the shared supervision of **Eurodac** were prepared (the EDPS supervises the central unit, while the national DPAs are responsible in their respective Member States). The EDPS was generally satisfied with the findings of the first phase of his inspections of the central unit.

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. The major developments of 2005 were:

- The issuing and implementation of a **paper on the advisory role** of the EDPS, which emphasises its wide scope (also covering the third pillar of the EU). This scope was subsequently confirmed by the Court of Justice. 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.
- The issuing of six formal **opinions**, clearly reflecting the relevant subjects on the policy agenda of the Commission, the Parliament and the Council. The most significant were:
  1. the exchange of personal data in the third pillar of the EU;
  2. 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
  3. the highly controversial subject of the mandatory retention of data on electronic communications for access by law enforcement authorities.
- Giving advice on **administrative measures**, in particular on implementing rules of institutions and bodies in the area of data protection.
- **Intervening before the Court of Justice** in the case of the transfer of PNR-data on airline passengers to the United States, in support of the conclusions of the Parliament which seeks to annul the related decisions of the Commission and the Council.

Co-operation

The EDPS's co-operative role covers not only data protection in the first pillar (EC Treaty), but also includes working together with national supervisory authorities and supervisory bodies in the third pillar of the EU; with the objective to improve consistency in the protection of personal data. The major developments of 2005 were:

- A certain number of important proposals for legislation were covered by the EDPS and the Article 29 Working Party in separate Opinions. In these cases, the EDPS welcomed the general support of national colleagues as well as additional comments which can lead to better data protection.
- Co-operation with the supervisory bodies for Schengen, Customs and Europol concentrated 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 co-operation between national supervisory authorities and the EDPS.
- The EDPS chaired several sessions in the context of the European and International Conferences of Data Protection Commissioners.

In co-operation with Council of Europe and OECD, the EDPS hosted a workshop on data protection in **international organisations**. Although often exempted from national laws, including laws on data protection, it is essential that international organisations nevertheless subscribe to the universal principles on data protection, especially so as they also often process sensitive data.

3.3. EUROPEAN DATA PROTECTION CONFERENCE

From 24-26 April 2005 the Spring Conference of European Data Protection Authorities took place in Cracow in Poland, organised by the Inspector General for the Protection of Personal Data, Ewa Kulesza. This year the Conference coincided with the tenth anniversary of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on free movement of such data. The basic topics for discussion included the reflection on the application and the interpretation of the Directive along with the adoption of a resolution concerning the protection of personal data in third pillar. Another issue commented on in this Conference was the transfer of the Data Protection Unit from the Direction General Internal Market of the European Commission to the Direction General Justice, Freedom and Security.

Chapter Four

Principal Developments in EEA Countries

Iceland

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

In 2005, a number of acts and administrative rules concerning data protection were passed. These are the most important ones:

1. *Act on the Governmental Gazette and the Legal Gazette, No. 15/2005. This act replaced Act No. 64/1943*. According to the new act, the aforementioned gazettes may be published on the Internet. The first one contains acts, regulations, other administrative rules, and international treaties and conventions. The latter one contains subpoenas, decisions on forced auctions, decisions on bankruptcy, etc. Thus, it is first and foremost the latter one that contains personal data. According to Article 7 of the act, the publishing on the internet shall, if possible, not lead to linking and further processing of personal data. The Icelandic Data Protection Authority, Persónuvernd, had pointed out in its Opinions on the matter that the creation of a database on individuals' financial matters, etc., accessible on the Internet, should be avoided. The aforementioned provision of the act is in accordance with that advice.

2. *Regulation on the Publishing of the Legal Gazette, No. 623/2005*. This regulation, which was passed by the Minister of Judicial Affairs, contains provisions on, amongst other things, how personal data should be protected in the Internet publication of this gazette, e.g. that individual advertisements (on decisions on forced auctions, etc.) should not be accessible to subscribers for longer than three years.

3. *Act No. 58/2005 Amending the Medicine Act, No. 93/1994, and the Act on Health Services, No. 97/1990*. This act is aimed at implementing the Bloodbank Directive, No. 2002/98/EC. In its opinion on the matter, Persónuvernd pointed out that a provision on the protection of personal data in bloodbanks, implementing Article 24 of the Directive, was lacking. Following this a provision was added, stating that Persónuvernd should monitor the processing of personal data in biobanks and that the processing should be in accordance with the Act on the Protection of Personal Data (No. 77/2000) and the Act on the Rights of Patients (No. 74/1997).

4. Act *No. 78/2005 Amending the Act on Telecommunications, No. 81/2003*. Amongst the provisions of this act is an amendment of Article 47 of the Telecommunications Act. According to this amendment, telecommunications companies are obliged to hand information on the users of IP numbers and telephone numbers over to the police even though the delivery of the information has not been ordered by a court. Persónuvernd criticised this provision in its Opinion on the matter.

5. *Rules on the Registration of Individuals Who Oppose to Their Names Being Used in Advertising and the Use of Such a Register, No. 36/2005*. These rules were passed by the Statistical Bureau of Iceland according to Article 28 of the Act on the Protection of Personal Data, No. 77/2000. They contain provisions stating further to the right granted in the aforementioned article to oppose being the object of direct marketing and, therefore, to be added to a register kept by the Statistical Bureau, which contains the names of those that oppose to this.

6. *Advertisement on the Transmission of Personal Data to Other Countries, No. 638/2005*. This advertisement, which was passed by Persónuvernd and is legally binding, replaced Advertisement No. 435/2003. It contains provisions on which third countries give personal data adequate protection, standard contractual clauses for the transfer of personal data to third countries, etc.

B. Major specific issues

None to report.

C. Major specific issues

One of the main tasks that Persónuvernd undertook in 2004 was inspections. Formal administrative decisions were taken regarding inspections that began in 2002 and 2003, i.e. on the lawfulness and security of the processing of personal data in two credit card companies and three life, accident and disease insurance companies. Only some minor faults were found concerning security. However, Persónuvernd made some major remarks on the lawfulness of the processing.

Thus, one of the credit card companies retained personally identifiable data on all credit card use by its customers from the time when it was founded, i.e. in 1980. Persónuvernd ordered the company to destroy data on individual transfers that were more than seven years old. Data on transfers that were younger than this could, however, be retained since it is stated in the bookkeeping legislation that all bookkeeping documents must be kept for seven years.

Also, Persónuvernd made some major remarks on the lawfulness of the processing of personal data by the insurance companies. Persónuvernd considered that before obtaining data on the health of an insurance applicant's relatives, the relatives should be asked for their consent. In the light of the new Act on Insurance Contracts, No. 30/2004, due to enter into force on 1 January 2006, Persónuvernd considered as well that after that time, it would be illegal to obtain data on relatives' hereditary diseases

Liechtenstein

Principal developments in third countries

The Data Protection Regulation (DSV) was reviewed again[39]: the revision, which was performed in close co-operation with the Data Protection Agency (DPA), stipulates that disclosure of identification data (first name, surname, address, date of birth) by the authorities is permissible in certain circumstances. The regulation also stipulates that the applicant must be explicitly informed at the disclosure of data that the details cannot be handed on and that they may only be used for the exclusive purpose stated in the application. If the disclosure entails a substantial effort for the authorities, a fee can be charged at an hourly rate of 100 Swiss francs. The second point involved creating a legal basis for the authorities concerning their practice of making various personal details known on their website during the process of a public invitation to tender. In practice, this involves disclosing the names and contact details of state employees or for instance the disclosure of federation members. It was determined here that specific further details (e.g. photographs of the persons concerned) could be disclosed, provided that the persons concerned were informed of this and agreed.

The DPA's opinions on legislative texts: in addition to the above-mentioned review of the DSV, the DPA was consulted on 15 other pieces of draft legislation. Two are given here:

- The legal basis for the national administration's central personnel administration (ZPV). This important draft legislation established in particular the legal foundation for a national identification number in the sense of Article 8 para. 7 of Directive 95/46/EC. The conditions under which this number may be used were also defined. Further aspects include the fact that an application procedure for data fields is planned. Legitimate data processing (in relation to individual data fields but also to the identification number) can only occur if the processing is lawful and proportionate and fulfils data protection requirements.
- Revision of the domicile document law to introduce biometrical passports. An Opinion was issued in keeping with various documents on the topic from the international sphere[40] and in particular encouragement was given to reinforcing the provision on the security of biometrical data in the law and also taking account of this in practice.

Specific topics: the check on applications for access entitlements to fields in the central personnel administration (ZPV), a centrally held Liechtenstein national administration database, was completed in mid-2005. Implementation of the permits then had to be reviewed. It was not possible to complete this substantial assignment by the end of the year.

The ZPV was developed before the entry into force of the DSG (data protection act) and in particular contains data on the entire permanent resident population. While it is possible to restrict access entitlements to certain fields, this is not the case for specific groups of people. Public offices, which work with the ZPV, require the data of those people with whom official contact exists. The data of all other persons is irrelevant for the office concerned. A restriction to certain groups of people is difficult to implement in view of the ZPV's given structure. Considerations on how this can nonetheless be achieved were still underway at the end of the reporting year.

[39] LGBl. 2005 no. 206

[40] Cf. e.g. WP 112

Information on current and/or important topics was provided on the Data Protection Agency's website www.sds.llv.li Of these the following are cited in brief: data-protection compliant handling of personal files, an updated list of third countries with equivalent data protection, biometrical data, RFID radio chips, a data protection guide to surfing in the workplace, a presentation on the topic 'Data protection – really something new in Liechtenstein?', another on 'Principles and application in research, the media and the Internet' and a decision on e-mail spam by the Swiss Data Protection Commission. The website was also expanded to include a new 'Press articles and interviews' section.

Finally, Directives on the topic 'Internet and e-mail supervision of the employee in the workplace' and 'Rights under the data protection law' were adopted and the Register of data collections was activated on the website at the end of the reporting year.

Norway

Significant changes to privacy or data protection law

None to report.

Significant changes to other laws affecting privacy or data protection

Changes in the Criminal Procedure Act

A number of amendments were made to the Criminal Procedure Act in 2005. These included the possibility for electronic room surveillance when given criteria. The possibility for mass surveillance of telephone numbers in one area to locate the telephone(s) used by a suspected person was also expanded

B. Major specific issues

None to report.

C. Major specific issues

Inspections

Biometric passports

On 3 October 2005, production of biometric passports was started in Norway. The Data Inspectorate has expended resources on this question during large parts of 2005. The background for this is the great uncertainty concerning security in connection with this passport, especially with a view to the possibilities for storage and reading. The Ministry of Justice has generally pointed out that international standards are the template for the security level of these passports. As of today, no such standards exist on which there is international agreement. The Data Inspectorate has therefore pointed out that it is highly unfortunate that the passport has been introduced before all security issues have been clarified. In comparison, both the USA and the UK have postponed its introduction.

Doping tests in sports

In 2005, the Data Inspectorate completed a project in which the processing of personal data in sports was assessed, both at top-level sports and in recreational and fitness sports. There was special focus on doping tests of athletes and amateur sportsmen, both in and outside organised sports. This project will be followed up in 2006.

The pilot project disclosed a need for a further review of the legal framework for doping tests and its relationship to privacy protection. An assessment must be made of whether consent is an appropriate basis for doping tests at all levels or whether such tests should be more clearly anchored in the statutory framework. A further demarcation is also needed between the areas in which doping tests may be accepted and areas where such tests must be considered as a disproportionate encroachment. The level and age of the athlete will be particularly relevant factors in this connection.

Working life

In 2005, the Data Inspectorate has dealt with a large number of cases concerning employers who had gone a very long way to control their employees. The Data Inspectorate chose to report some of these cases to the Police, after having conducted an inspection. Two of the

cases concerned employers who had retained all e-mails their employees sent or received at work, also private e-mails, without notifying their employees that this could happen. One of the cases concerned an employer who installed a hidden surveillance camera in a locker room to expose employees who were stealing. A fourth case concerned a bank using pictures from its surveillance camera system to check whether the cleaner was doing a proper job, which was not the objective of the bank's surveillance camera.

Consultations

New employment and welfare administration

To offer better incentives to get persons receiving social security benefits back to work and to reduce the group of persons needing support who for various reasons fall outside the scope of welfare schemes, the Government and the Storting wanted a coordination of government services in the areas of employment, social security and social welfare. The Data Inspectorate criticised the proposed bill on the employment and welfare administration, considering that it had too many shortcomings in the area of privacy protection. In addition, both the Data Inspectorate and the Norwegian Board of Health pointed out that the confidentiality provisions were ambiguous and difficult to understand.

The Data Inspectorate fears the risk that the new employment and welfare administration will allow all case officers to share information about all of us, without giving the individual a chance to know where all this information is going.

To arrive at an acceptable solution, a number of principles must be followed, among them: nobody should have access to more personal data than that which is needed for the proper performance of work tasks. Any inquiry made by an employee must be logged, and the logs must be controlled. The Data Inspectorate's impression is that no plans have been made to limit the information each case officer will have access to in the data systems. This means that each case officer's duty of confidentiality and integrity will in reality constitute the only guarantee for privacy protection, while at the system and official level, most inappropriate inquiries may be written off as "human failure".

Proposal for a new Immigration Act

The proposal for a new Immigration Act raises many issues affecting privacy protection. One of the main questions is what information should be accessible to the immigration authorities in their assessment of whether a person should be granted various types of residence permits. Another central issue is what data may be collected about a person resident in Norway, a so-called "reference person", who applies for a visitor's visa for a foreign national. In the Data Inspectorate' opinion, the Immigration Act Committee has clearly gone too far in proposing personal checks on reference persons. The Data Inspectorate believes that the bill opens up too many possibilities for collecting data, both character references and unconfirmed data. It will be difficult to submit unconfirmed data, such as information provided in confidence at a crisis centre, to a reference person, and such information will therefore be impossible to refute.

Criminal record certificates

The Data Inspectorate has submitted a number of consultative statements in which the subject was the requirement to present criminal record certificates. This has been an issue for both occupational categories and the voluntary sector. The Data Inspectorate believes there is reason to ask whether adequate protection is ensured when obtaining such a certificate, or if such a measure could just as well result in a false sense of security. This issue is sensitive, and the Data Inspectorate has in these cases underlined the importance of not adopting comprehensive measures that will contribute to a false sense of security. In most of the consultation papers received, the description of the problem at hand was highly inadequate.

The Data Inspectorate observes that there is an increasing number of occupations where criminal record certificates are required, and is not surprised that this trend should also be spreading to the voluntary sector. This trend could easily increase and will perhaps be impossible to reverse at present. The main justification for requiring a criminal record certificate to be presented in various sectors and for different occupational groups is precisely that such certificates are required in other areas, and that a sector in which a criminal record certificate is not required may consequently attract unsuitable persons not admitted elsewhere. The Data Inspectorate warns against a development in which participation in most arenas of society requires prior police clearance.

Decisions and clarifications

Testing for intoxicants

In the beginning of 2006, the Data Inspectorate's complaints commission, the Privacy Appeals Board, reached a conclusion in a case concerning the testing of employees in a security firm for intoxicants. Pursuant to Norwegian law, an employer may only require testing for intoxicants when this follows from law or regulations, in positions entailing special risks or when the employer considers it necessary to protect life or health. Some occupational groups, such as seafarers, have a statutory obligation to accept such tests. However, this does not apply to employees in security services companies. The Privacy Appeals Board concluded that the security firm did not have the right to test all employees regardless of the work they were meant to perform.

Freedom of expression on the Internet

A group that felt it had been subjected to abuse by authority in connection with some child welfare cases published personal characterisations on the Internet of players that had been working with such cases. The Personal Data Act has important exemptions from various requirements to the use of personal data for "opinion-forming" activities. The persons concerned regarded the information about them to be both incorrect and defamatory. The Data Inspectorate dismissed the case on the grounds that an encroachment on the freedom of expression is

so serious that it requires a clear legal authority, and that the authority of the Personal Data Act was not sufficiently clear. The persons in question appealed against this decision to the Privacy Appeals Board. The Board accepted that the Internet pages were opinion forming, but did not allow the appeal.

Deleting sound recordings

A person was refused access to personal data stored on sound recordings of telephone conversations he had taken part in. The Privacy Appeals Board came to the conclusion that the case lay outside the scope of the Personal Data Act. In this connection, the Board came to a decision on whether the sound taping had been carried out with electronic appliances or not. It was concluded that if the recording was started and stopped manually, it could not be considered as having been performed with an electronic appliance, even if the recorder must technically be characterised as electronic, and regardless of whether the recording was digital or analogous.

Mapping of attitudes

Studies on privacy protection and privacy legislation

In 2005, The Data Inspectorate and the Ministry of Government Administration and Reform arranged for a privacy protection survey in the population and among businesses. In general, this survey revealed that the population is generally not very concerned about misuse of personal data, and that most people think business enterprises act reasonably. However, when businesses were questioned, it turned out that this trust may perhaps be a little misplaced. Businesses have a positive view of privacy protection, but very few of them work systematically with such questions. Moreover, most businesses possess very little knowledge about the Personal Data Act.

Chapter Five

Members of the Article 29 Data Protection Working Party in 2005

MEMBERS IN 2005

Austria	**Belgium**
Frau Dr Waltraut Kotschy Österreichische Datenschutzkommission Ballhausplatz 1 - AT - 1014 Wien Tel: +43 1 531 152679; +43 1 531 152525 Fax: +43 1 531 152690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Monsieur Michael Parisse Président Commission de la protection de la Vie privée Rue Haute, 139 - BE - 1000 Bruxelles Tel: +32 2 213.85.40 Fax: +32 2 213.85.65 E-mail: commission@privacycommission.be Website: http://privacycommission.be
Cyprus	**Czech Republic**
Ms Goulla Frangou Commissioner for Personal Data Protection 40, Themistokli Dervi str. Natassa Court, 3rd floor - CY - 1066 Nicosia or P.O. Box 23378 - CY - 1682 Nicosia Tel: +357 22 818 456 Fax: +357 22 304 565 E-mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy	Mr Igor Nemec President Office for Personal Data Protection Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tel: +420 234 665 281 Fax: +420 234 665 501 E-mail: info@uoou.cz Website: http://www.uoou.cz/
Denmark	**Estonia**
Ms Janni Christoffersen Director Datatilsynet Borgergade 28, 5th floor - DK - 1300 Koebenhavn V Tel: +45 33 193236 Fax: +45 33 193218 E-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk	Mr Urmas Kukk Director General Estonian Data Protection Inspectorate Väike - Ameerika 19 - EE - 10129 Tallinn Tel: +372 6274 135 Fax: +372 6274 135; +372 6274 137 E-mail: urmas.kukk@dp.gov.ee; info@dp.gov.ee Website: http://www.dp.gov.ee
Finland	**France**
Mr Reijo Aarnio Data Protection Ombudsman Office of the Data Protection Ombudsman P.O. Box 315 - FI - 00181 Helsinki Tel: +358 10 36 66700 Fax: +358 10 36 66735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi	Mr Georges de La Loyere Commissaire en charge du secteur international Commission Nationale de l'Informatique et des Libertés (CNIL) Rue Vivienne, 8 - FR - 75002 Paris Tel: +33 1 53 73 22 31; +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-mail: laloyere@cnil.fr Website: http://www.cnil.fr

Germany	**Greece**
Herr Peter Schaar Chairman Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Herr Peter Schaar Husarenstraße 30 - DE -53117 Bonn Tel: +49 228 81995 0 (Poststelle) Tel: +49 228 81995 100 (direct) Fax: +49 228 81995 550 E-mail: peter.schaar@bfdi.bund.de Website: http://www.bfdi.bund.de	Mr Nikolaos Frangakis Advocate Member of the Hellenic Data Protection Authority Kifisias Av. 1-3, PC 115 23 Ampelokipi - GR - Athens Tel: +30 210 64.75.601, +30 210 36.32.671 Tel: +30 210 64.75.629, +30 210 64.75.679 Fax: +30 210 33.52.617, +30 210 36.31.631 +30 210 64.75.728 E-mail: info@sofralaw.gr Website: http://www.dpa.gr
Hungary	**Ireland**
Dr Attila Peterfalvi Parliamentary Commissioner Office of Parliamentary Commissioners Nador u. 22 - HU - 1051 Budapest Tel: +36 1 475 7186; +36 1 475 7100 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Website: http://abiweb.obh.hu	Mr Billy Hawkes Data Protection Commissioner Irish Life Centre, Block 6 Lower Abbey Street - IE - Dublin 1 Tel: +353 1 8748544 Fax: +353 1 8745405 E-mail: info@dataprotection.ie Website: http://www.dataprotection.ie
Italy	**Latvia**
Professor Francesco Pizzetti Président Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 - IT - 00186 Roma Tel: +39 06 69677403 Fax: +39 06 69677405 E-mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it	Ms Signe Plumina Director Data State Inspectorate Kr. Barona Street 5-4 - LV - 1050 Riga Tel: +371 722 31 31 Fax. +371 722 35 56 E-mail: info@dvi.gov.lv Website: http://www.dvi.gov.lv
Lithuania	**Luxembourg**
Mr Algirdas Kun inas Director State Data Protection Inspectorate Gedimino Ave 27/2 - LT - 01104 Vilnius Tel: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-mail: ada@ada.lt Website: http://www.ada.lt	M. Gérard Lommel Président Commission nationale pour la Protection des Données 41, avenue de la Gare - LU - 1611 Luxembourg Tel: +352 26 10 6020 Fax: +352 26 10 6029 E-mail: info@cnpd.lu Website: http://www.cnpd.lu

Malta	**The Netherlands**
Mr Paul Mifsud Cremona Data Protection Commissioner 2, Airways House High Street - MT - SLM 16 Sliema Tel: +356 2328 7100 Fax: +356 23287198 E-mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt	Mr Jacob Kohnstamm College Bescherming Persoonsgegevens (CBP) Dutch Data Protection Authority Juliana van Stolberglaan 4-10 Postbus / P.O. Box 93374 NL - 2509 AJ Den Hague / The Hague Tel: +31 70 8888.500 Fax: +31 70 8888.501 E-mail: info@cbpweb.nl Website: http://www.cbpweb.nl; www.DutchDPA.nl
Poland	**Portugal**
Ms Dr Ewa Kulesza Inspector General for Personal Data Protection Bureau of the Inspector General for Personal Data Protection ul. Stawki 2 - PL - 00193 Warsaw Tel: +48 22 860 70 81; +48 22 860 73 12 Fax: +48 22 860 70 90 E-mail: sekretariat@giodo.gov.pl; dp@giodo.gov.pl Website: http://www.giodo.gov.pl	Mr Luís Da Silveira Président Comissão Nacional de Protecção de Dados Rua de São Bento, 148, 3o PT - 1 200-821 Lisboa Codex Tel: +351 21 392 84 00 Fax: +351 21 397 68 32 E-mail: geral@cnpd.pt Website: http://www.cnpd.pt
Slovakia	**Slovenia**
Mr Gyula Veszelei President Office for the Personal Data Protection of Slovakia Odborarska namestie 3 - SK - 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441 E-mail: statny.dozor@pdp.gov.sk ; gyula.veszelei@pdp.gov.sk Website: http://www.pdp.gov.sk	Mrs Natasa Pirc Musar Information Commissioner Vosnjakova 1, SI - 1000 Ljubljana Tel: +386 1 230 97 30 Fax: +386 1 230 97 78 E-mail: gp.ip@ip-rs.si Website: http://www.ic-rs.si , http://www.ip-rs.si

Spain	**Sweden**
Mr José Luis Piñar Mañas Vice Chair Director Agencia de Protección de Datos C/ Jorge Juan, 6 ES - 28001 Madrid Tel: +34 91 399 6220 Fax: +34 91 447 1092 E-mail: director@agpd.es Website: http://www.agpd.es	Mr Göran Gräslund Director General Datainspektionen Fleminggatan, 14 (9th Floor) Box 8114, SE - 104 20 Stockholm Tel: +46 8 657 61 00; +46 8 657 61 57 Fax: +46 8 650 86 13; +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se ; goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
United Kingdom	**European Data Protection Supervisor**
Mr Richard Thomas Information Commissioner Information Commissioner's Office Wycliffe House Water Lane - GB - SK9 5AF Wilmslow Tel: +44 1625 545700 Fax: +44 1625 524510 E-mail: pdq@ico.gsi.gov.uk; mail@ico.gsi.gov.uk Website: http://www.informationcommissioner.gov.uk	Mr Peter Hustinx European Data Protection Supervisor Postal address: 60, rue Wiertz, BE - 1047 Brussels Office: rue Montoyer, 63, BE - 1047 Brussels Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

OBSERVERS OF THE ART. 29 DATA PROTECTION WORKING PARTY IN 2005

Iceland	**Norway**
Ms Sigrun Johannesdottir Director Icelandic Data Protection Authority Raudararstigur 10 - IS - 105 Reykjavik Tel: +354 560 9010; +354 510 9600 Fax: +354 510 9606 E-mail: postur@personuvernd.is Website: http://www.personuvernd.is	Mr Georg Apenes Director General Datatilsynet The Data Inspectorate P.B. 8177 Dep - NO - 0034 Oslo Tel: +47 22 396900 Fax: +47 22 422350 E-mail: postkasse@datatilsynet.no Website: http://www.datatilsynet.no
Liechtenstein	**Bulgaria**
Herr Dr Philipp Mittelberger Data Protection Commissioner of the Principality of Liechtenstein Aeulestrasse 51 - LI - 9490 Vaduz Tel: +423 236 6090/91 Fax: +423 236 6099 E-mail: info@sds.llv.li Website: http://www.sds.llv.li; http://www.liechtenstein.li	Mr Ivo Stefanov Commission for Personal Data Protection (CPDP) 1 Bvld Dondukov - BG - 1000 Sofia Tel: +359 2 940 2046 E-mail: kzld@government.bg
Romania	
Mrs. Georgeta Basarabescu President National Supervisory Authority for Personal Data Processing Olari Street no. 32, 2nd district, RO - Bucharest Tel: +40 21 252 5599 Fax: +40 21 252 5757 E-mail: georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Website: www.dataprotection.ro	

Secretariat of the Art. 29 Working Party
Mrs Niovi Ringou Acting Head of unit Data Protection Unit Directorate-General Justice, Freedom and Security European Commission Office: LX46 01/53 - BE - 1049 Brussels Tel: +32 2 296 3037 Fax: +32 2 299 8094 E-mail: Niovi.Ringou@ec.europa.eu Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm