Tenth Annual Report

of the Article 29 Working Party on

Data Protection

EUROPEAN
COMMISSION

1830-6446

Tenth 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 2006

Adopted in June 2007

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

The protection of personal data is of vital importance for a democratically healthy information society. Data protection is, thus, one of the most important civil rights of the 21st century. In over ten years of existence, the Working Party, according to Article 29 of the European Data Protection Directive 95/46/EC, has evolved into one of the most relevant co-operation committees in the area of data protection in Europe, dealing with a large variety of legal and technological issues.

The following subjects dominated the work of the Article 29 Working Party in 2006, the year under report:

- For the first time in Europe an initiative, in close co-operation with all European Member States, has been launched to monitor the application and implementation of legal provisions in the light of data protection law.
- As before, the effective protection of privacy is at stake when governmental bodies intend to use personal data, initially collected by private companies within the framework of their customer relationship, in the area of law enforcement. This concerns, for example, data generated when booking a flight or when carrying out cross-border bank transfers. A major concern is that, up until now, there has been no instrument in the area of community law in place regulating data protection in the third pillar, i.e. in the field of justice and law enforcement.
- When it comes to further developing electronic services and to opening up new areas of application of telematics, data protection aspects have to be taken into account as early as possible. The Article 29 Working Party also focused its attention on the monitoring and supporting of such projects.

The first European-wide audit, aimed at a harmonised implementation of the EC Data Protection Directive in the EU Member States and carried out at health insurance companies, underlines the importance of joint action by national supervisory authorities. After consultation with the European Insurance and Reinsurance Federation (CEA), this sector has been singled out for two reasons: it concerns a very large part of the population and it collects particularly sensitive personal data. The Article 29 Working Party takes the view that such an audit is of great importance to all parties concerned. It shows that the supervisory authorities of the EU Member States not only closely co-operate in such a highly sensitive area, but that they also manage to impose jointly developed positions in the field of data protection. For the companies concerned, this joint effort has stressed that data protection provisions are being implemented in a harmonised way in the European common area. For the persons insured, this action has raised their awareness of data protection by giving them more information about their rights.

After the European Court of Justice's decision of 30 May 2006 ruling that the agreement concluded between the EU and the USA in May 2004 on the transfer of passenger name record

(PNR) data had to be annulled at the end of September 2006 at the latest due to the lack of a legal basis, a follow-up agreement valid until 30 July 2007 was negotiated in October 2006. In principle, the conclusion of this follow-up agreement has to be welcomed, as otherwise there would not have been any legal basis for the transfer of PNR data to the US Department of Homeland Security, and the air passengers' rights and civil liberties would henceforth not have been guaranteed. Before that follow-up agreement, the Article 29 Working Party spoke out against the conclusion of bilateral agreements, otherwise there would have been a risk of non-harmonised implementation of the European Data Protection Directive and weaker passenger rights would have ensued. During the negotiations about the new agreement, it was agreed that the undertakings given in 2004 by the USA when concluding the treaty remain valid. However the reservations regarding vital points of the agreement which the Article 29 Working Party voiced during the conclusion of the first PNR agreement remain. They concern, in particular, the purpose limitation and also the amount of data that has to be transferred. As before, the US authorities obtain data in the so-called 'pull-system', which means that by accessing the airlines' reservation systems they get access to the complete data record available for each individual passenger. The first PNR agreement of 2004 envisioned the shift from the 'pull-system' to an active so-called 'push-system' which allows, in addition to reducing the data record to a maximum of 34 data elements, for sensitive data to be filtered out by using a filtering software. The European airlines have repeatedly stated that the requirements for transmitting data by pushing them are now given so there are no plausible reasons for any further delay. For that reason, during the past year, the Article 29 Working Party repeatedly called on the contracting parties to realise the 'push' solution immediately.

The other main issue for the Article 29 Working Party was the US authorities' access to payment transactions data processed by SWIFT (Society for Worldwide Interbank Financial Telecommunication) for the purpose of fighting terrorism. SWIFT is an industrial co-operative under Belgian law founded in 1973 by international banks. The payment orders forwarded by the SWIFTNet FIN Service contain personal data, such as the name of the sender and the addressee. SWIFT stores all money transfer data for 124 days in two computer centres; one is situated in Europe, the other in the USA. Since 2001, based on governmental subpoenas, American authorities have repeatedly enforced the disclosure of transaction data by SWIFT. In this context, the technical point of contact for these orders was the SWIFT computer centre located in the USA. SWIFT has disclosed data without any previous judicial review. In 2003, SWIFT and the US authorities concluded an agreement laying down the procedure for data transfers. In general, SWIFT users have not been informed about the fact, the scope and the purpose of such transfers. Last year, the Article 29 Working Party found out that, pursuant to European data protection law, the whole procedure is inadmissible due to a non-existing legal basis. In particular, the USA does not have an adequate level of data protection according to section 25 paragraphs 1 and 2 of Directive 95/46/EC. The legal responsibility for data transfers to the USA lies within both SWIFT and those banks using SWIFT's services. The Article 29 Working Party called upon the banks to immediately propose measures by which a data transfer to the USA

can either be stopped or at least the transferred data records be sufficiently secured against undue access. According to section 10 and 11 of the EU Data Protection Directive, all banks in the EU, including central banks using the services of SWIFTNet Fin Service, have to make sure that their customers are adequately informed about the processing of their data and about their rights in this respect. Furthermore, the customers must also be informed about the fact that US authorities can access their data.

In view of the intensified co-operation among European security authorities, a common Europe-wide standard for data protection is also indispensable in this area. From a data protection point of view, the Hague Programme, adopted in 2004 by the heads of state and government, is of crucial importance. This programme aims to strengthen liberty, security and justice in the EU by laying down guidelines in the area of home affairs and judicial policy for the period from 2005 to 2010. Thus, from 1 January 2008 onwards, the exchange of information relevant for law enforcement purposes shall be based on the principle of availability. However, this only applies in the EU Member States if there exists, on the one hand, a common standard for data protection guaranteeing the integrity and confidentiality of data exchanged in such a way and on the other, an effective control of data protection. Subsequently, in October 2005, the Commission presented proposals for framework decisions on the exchange of information based on the availability principle and for the protection of personal data processed within the framework of police and judicial co-operation in criminal matters. Concerning the proposed new legal instrument on the protection of personal data processed within the framework of police and judicial co-operation in criminal matters, the Commission closely followed the EU Data Protection Directive, and in doing so took the requirement of the European Data Protection Conference into account, demanding the development, as far as possible, of data protection rules for the third pillar which correspond to the current level of data protection in the first pillar. By providing harmonised standards indicating how personal data should be collected and processed by the police and law enforcement authorities of the EU Member States, and how the right of informational self-determination of the persons concerned by the processing is guaranteed, a framework decision on data protection would contribute to the harmonisation of the procedure and promote the mutual confidence which is necessary for cross-border information exchanges. Therefore, a framework decision on data protection would facilitate the cross-border exchange of data. The framework decision should cover the whole information process at national police and law enforcement authorities, and also between Member States and third countries when exchanging information. The objective is a far-reaching harmonised data protection standard for information processing by police and judicial authorities within the whole EU in order to avoid any divergence of current applicable data protection regulations. In particular, the fundamental principles of purpose limitation, data quality and necessity have to be respected. When processing information, the data subjects' rights have to be guaranteed on a basis that is as harmonised as possible. Apart from an independent data protection control in every Member State, it has to be made sure that the Council of the European Union gets independent advice from representatives of the national data protection authorities.

In the past year, the Article 29 Working Party also put great emphasis on a continuous dialogue with representatives from the business sector and with other stakeholders; for example, it consulted the public before adopting the Opinion on RFIDs (Radio Frequency Identification) (WP 105). The procedural method used when applying so-called Binding Corporate Rules (BCR) has also been discussed with representatives of the business sector. These rules aim to facilitate considerably the framework of personal data to countries without an adequate level of data protection. Europe-wide harmonised BCR-application forms are expected to be finalised in spring 2007. Other important subjects were the duty of companies to adequately inform their customers about their data protection rights (so-called Short Privacy Notices), the protection of intellectual property rights and data protection aspects when it comes to so-called 'whistle blowing' in the fight against corruption and falsification of accounts.

Also in 2006, the ever-increasing development of information technology made it necessary to put the instruments of data protection to the test and adapt them where necessary. For the future it remains important that, in the interest of all data subjects, further legal and practical steps are taken in order to achieve a high-level harmonisation of data protection, and, in particular, governmental responses to security threats should not result in unacceptable restrictions in civil liberties or infringements of the established data protection legislation.

Peter Schaar

Chapter One

Issues Addressed by the Article 29 Data Protection Working Party[1]

[1] 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

1.1. PASSENGER DATA / PNR

Opinion 4/2006[2] on the Notice of proposed rule making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71).

This opinion is a reflection on the new US legislative proposal concerning the collection of passenger information by air carriers and shipping lines for the control of communicable diseases (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71). It examines carefully the foreseen regulations and analyses them not only in the light of the EU-Directive Data Protection 95/46/EC but also in the light of the WHO International Health Regulations (2005) which is non-binding in its nature but intends to support nations in their fight against communicable diseases.

Opinion 5/2006[3] on the ruling by the European Court of Justice of 30 May 2006 in Joined cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States.

The present opinion is issued after the ruling by the European Court of Justice of May 30 2006 which annuls both the Commission Decision on the adequacy finding and the Council Decision on the conclusion of the PNR Agreement and which obliges the Community Institutions to terminate the Agreement with the United States on the transfer of passenger data. With this opinion, the WP urges the timely adoption of a new agreement between the US and EU before the deadline in order to avoid any legal gaps and to ensure the rights and freedoms of passengers continue to be protected at least at the present level. The opinion also concludes that the Court ruling shows once more the difficulties arising from the artificial division between the pillars and the need for a consistent cross pillar data protection framework.

Opinion 7/2006[4] on the ruling by the European Court of Justice of 30 May 2006 in Joined cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement.

With this opinion, the WP expresses its concerns one more time at the risk of the absence of an agreement with the US on the transfer of passenger data (see Opinion WP 122). It stresses that whilst the judgement of the European Court of Justice of resulted in the annulment of the agreement with the US, it does not affect the obligations to comply with data protection requirements under national law. For this reason, it considers that the continued compliance with the Undertakings is of the utmost importance. It reiterates its hope for concluding a new satisfactory agreement so as to make consideration of enforcement actions by national data protection supervisory authorities unnecessary.

Opinion 9/2006[5] on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data.

In this Opinion, the WP fully supports the objective of curbing illegal immigration by improving checks on EU-bound flights as set out in Council Directive 2004/82/EC. However,

[2] WP 121
[3] WP 122
[4] WP 124
[5] WP 127

it is keen to ensure that the transposition of this Directive into national law takes place in as harmonised and consistent a manner as possible by taking account of the data protection principles enshrined in Directive 95/46/EC. For that reason, in this Opinion the WP sets out some implementing and interpretive guidelines in order to prevent diverging approaches by Member States that might result from the lack of clear-cut indications in some provisions of the Directive in question. The WP calls upon the legislatures of Member States and all competent national authorities to take into account these guidelines in developing and applying national legislation transposing the Directive.

1.2. ELECTRONIC COMMUNICATIONS, INTERNET AND NEW TECHNOLOGIES

Opinion 2/2006[6] on privacy issues related to the provision of email screening services.

Aware of the expansion of different on-line based communication services, including free web-based email services and related services, the WP is concerned about the protection of the privacy of the communications, in particular because of existing practices to inspect communications in order to eliminate spam and viruses as well as to detect any predetermined content. The WP is aware that most of internet and email service providers use filtering tools to protect networks and machines as well as, in fewer cases, to inspect communications for commercial reasons. However the WP considers that, in some cases, using such filtering tools may not be in compliance with the existing data protection legislation, whose application is not always clear to these new types of services. The main purpose of this paper is to provide guidance on the question of confidentiality of email communications and, more specifically, on the filtering of on-line communications. To this end, this paper analyses, among others, the provisions on confidentiality of the e-communications as defined in Article 5 paragraph 1 of the 2002/58 Directive on privacy and electronic communications as well as other relevant provisions that are part of the acquis communautaire and national laws implementing it. It encourages email service providers to take into account the guidelines and recommendations contained in the Opinion in the provision of their services.

Opinion 3/2006[7] on the Directive 2006/24/EC of the European Parliament of the Concil on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

On 15 March 2006 the Council adopted Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks services and amending Directive 2002/58/EC. The WP notes that the Directive lacks some adequate and specific safeguards as to the treatment of communication data and leaves room for diverging interpretation and implementation by the Member States in this respect and in order to transpose the provisions of the Directive in a uniform way and to comply with the requirements of Article 8 of the European Convention on Human Rights, Member States should implement safeguards. This paper establishes the safeguards that should be taken into account.

[6] WP 118

[7] WP 119

Working document[8] on data protection and privacy implications in eCall initiative.

The aim of this working document is to outline data protection and privacy concerns arising in connection with the planned introduction of a harmonised pan-European in-vehicle emergency call ("eCall") service that builds on the single European emergency number 112. The WP recognises the socio-economic benefit that the wide introduction of the eCall service might bring to citizens, but the deployment of the eCall service has privacy and data protection implications that have to be emphasized and properly addressed. The WP, while identifying privacy concerns related to the eCall, privileges and recommends the voluntary approach for the possible introduction of the eCall service. From a data protection point of view, an emergency call released automatically by a device or triggered manually and transmitted via mobile networks resulting in geolocalization of the emergency event is in principle admissible, provided that there exists a respective specific legal basis and sufficient data protection safeguards are provided.

Opinion 8/2006[9] on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive.

With this Opinion the WP expresses its concerns and comments on the review of the eCommunications package, in particular on the ePrivacy Directive It also refers to its Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector where various proposals were suggested but not reflected. In the present Opinion Working Party enumerates them again. It also wishes to recommend improvement of security measures and to emphasize that protection of users and creating their trust into eCommunications should be seriously taken into account while improving the security of infrastructure. The WP also suggests that the issues surrounding online applications (security concerns, responsibility by the operators as well as clarification of both legal status and of the data controller.) should be addressed.

1.3. SWIFT

Opinion 10/2006[10] on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

This opinion of the Article 29 Working Party contains the findings on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). In this context, the Article 29 Working Party emphasizes that fundamental rights must remain guaranteed even in the fight against terrorism and crime. It insists therefore on the respect of global data protection principles. The opinion publishes some conclusions that the WP intends to follow-up and monitor.

1.4. ACCOUNTING, AUDITING AND FINANCIAL MATTERS

Opinion 1/2006[11] on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

[8] WP 125
[9] WP 126
[10] WP 128
[11] WP 117

This opinion provides guidance on how internal whistleblowing schemes can be implemented in compliance with the EU data protection rules enshrined in Directive 95/46/EC. It considers that compliance with the principles of protection of personal data helps companies and whistleblowing schemes to ensure the proper functioning of such schemes. It also considers essential that in the implementation of a whistleblowing scheme the fundamental right to the protection of personal data, in respect of both the whistleblower and the accused person, be ensured throughout the whole process of whistleblowing. The WP stresses the principles of data protection, as laid down in Directive 95/46/EC, must be applied in full to whistleblowing schemes, in particular with regard to the rights of the accused person to information, access, rectification and erasure of data. However, given the different interests at stake, the WP recognises in the document that application of these rights may be the object of restriction in very specific cases, in order to strike a balance between the right to privacy and the interests pursued by the scheme. However, any such restrictions should be applied in a restrictive manner to the extent that they are necessary to meet the objectives of the scheme.

1.5. MAINTENANCE OBLIGATIONS

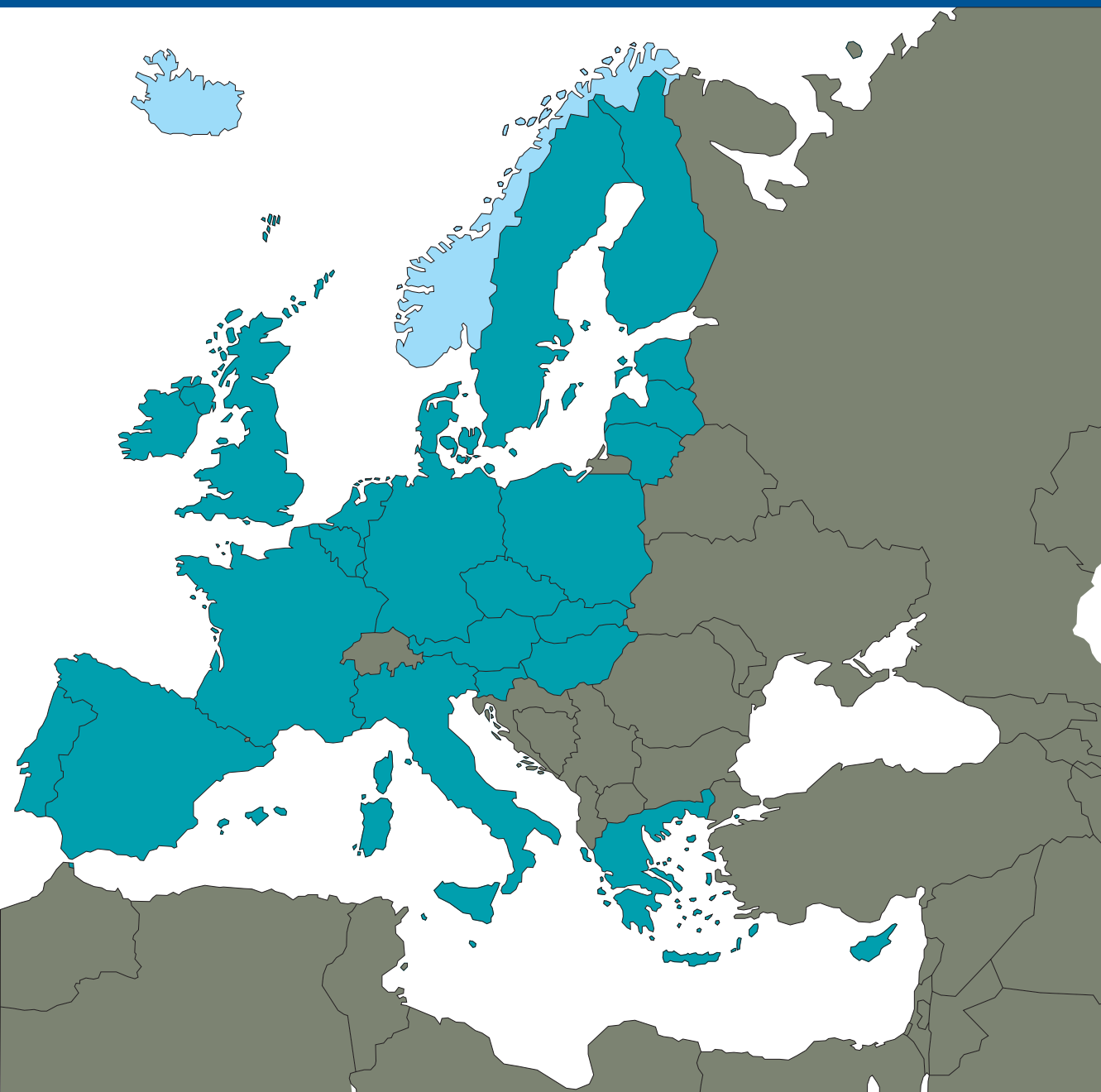
Opinion 6/2006[12] on the Proposal for a Council Regulation on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations.

In this document the WP raises a number of data protection issues on the Commission Proposal for a Council Regulation on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations, in particular, on Chapter VIII ("Cooperation") which includes a mechanism involving the collection of information about the situation of the creditor and the debtor and its exchange through a network of national central authorities. The Opinion reminds that such data processing must comply with the principles and rules laid down in the Directive. It notes that the proposal already contains a number of elements aimed at ensuring compliance of the data processing operations with those principles and identifies other points where additional data protection safeguards should be built into the system of exchange of personal data.

[12] WP 123

Chapter Two

Main Developments in Member States



Austria

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

The directive 2004/48/EC on the enforcement of intellectual property rights has been implemented, permitting copyright holders to obtain personal data of copyright violators more easily. This is especially relevant for the data of Internet users who are suspected of swapping music online. The directive was adopted into the Austrian copyright law *(Urheberrechtsgesetz)* with an amendment published in the Federal Law Gazette I No. 81/2006 on 21 June 2006.

The Austrian Police Act *(Sicherheitspolizeigesetz)* was amended (cf. Federal Law Gazette Part I No. 158/2005) giving the police additional powers to protect state visits and sports events. Extended possibilities of using data from video surveillance, operated by private parties, are included.

The Act concerning the Execution of Legal Titles *(Exekutionsordnung)* was amended to protect the privacy of people who suffer from undesired contact or other attention (cf. Federal Law Gazette Part I No. 56/2006). The new section 382g of the Exekutionsordnung permits a court to forbid a party to use personal data of another party in a manner that is designed to violate privacy or to harass (e.g. posting personal data on the Internet to defame him or her).

B. Major case law

1) An Austrian Internet service provider (ISP) kept records about a customer's dynamic IP address to enforce a 'fair use' policy on data transfer volume. The ISP was compelled to disclose this data by court order to a copyright collecting agency. Two customers who were subsequently accused of copyright piracy filed this complaint against the ISP for illegally keeping this data. The Austrian Telecommunication Act (Telekommunikationsgesetz 2003 – TKG 2003, Federal Law Gazette I No. 70/2003), which regulates what data may be kept by ISPs, rules in sect. 99 para. 1 that all traffic data have to be deleted after the session ends. The data protection commission has ruled that the ISP had no right to keep the dynamic IP addresses for billing purposes longer than was actually needed, as dynamic IP addresses are traffic data.

2) A sanatorium had permission for a helicopter-landing pad, under the assumption that the number of flights would be less than ten per winter season. A group of citizens in the neighbourhood believed that the actual number of flights was much higher. They found the helicopter noise intolerable and decided to document landings by means of video cameras. A complaint procedure was filed by a helicopter pilot and the commission ruled that the videotapes would fall under the definition of data processing and were thus basically subject to the right of access, provided that the intention of taking the photos was surveillance of individuals. As the recordings were not intended to identify the pilot or other data subjects but merely to document the number of helicopter flights, the commission ruled that no right of access existed because the data subject (the pilot) could not reasonably be identified.

3) A railway company operated railways cars equipped with video cameras, but the cameras were not in use pending approval by the data

protection commission in a 'prior checking' procedure. A citizen who rode in one of these cars demanded right of access. The commission ruled that as the data collection equipment was not in use it did not qualify as a 'data application', and therefore the railway company did not have to grant any right of access.

4) Another case involved a citizen whose personal data appeared in a document submitted to the Austrian Parliament, which was then published on the Parliament's website. Following a complaint by the citizen to Parliament, his name was anonymised. However, as Internet search engines still found the indexed document, he complained to the data protection commission, which ruled that the Parliament could not be held responsible for search engines.

C. Major specific issues

Video surveillance

The number of notifications of and complaints about video surveillance has dramatically increased over the last year. This is due to a heightened perception in the public as well as an organised policy to arrange for better notification.

Trans-border data flows

The Austrian data protection commission has observed that most international corporations wishing to transfer data to countries without an adequate level of data protection use the standard contractual clauses as the preferred legal instrument. Few corporations based in the USA use the 'Safe Harbor' agreement, even though the office of the data protection commission routinely informs corporate representatives and their lawyers about this option. Requests to specify the reasons for not using the Safe Harbor agreement remain unanswered.

The corporations are equally slow to adopt Binding Corporate Rules (BCR), but the office of the data protection commission has observed several attempts to construct BCR-like systems using modified versions of the standard contractual clauses.

Belgium

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

Directive 95/46/EC and Directive 2002/58/EC

No provision.

Other legislative developments

Coordinating Body for Threat Analysis (OCAM)
The Act of 10 July 2006 on the analysis of threats (*Belgian Monitor*, 20 July 2006) set up a new body, the Organe de Coordination pour l'Analyse de la Menace (OCAM), charged with evaluating terrorist and extremist threats that could compromise the internal and external security of the State, and Belgian interests and the security of Belgian nationals abroad. In order to carry out its missions, the OCAM may create one or more databases, the purposes, data and information categories, data-retention periods, access and communication, and erasure procedures of which are determined by a Royal Decree, deliberated by the Council of Ministers, after consultation with the Belgian Commission.

One draft Royal Decree was submitted for the Belgian Commission's opinion, which expressed its reservations on the 30-year data-retention period. It is also of the opinion that the necessity to store data should be subject to regular assessment. It further points out that data relevance should be verified on a case-by-case basis whenever data is used and overall every five years. Finally, the Commission points out that, given the legal deficiencies identified in the legal framework surrounding the body which the OCAM is to replace, that body's access to data through various information systems does not imply OCAM's legality of access to the same systems.

This Royal Decree was adopted on 28 November 2006. Only some of the Commission's observations were taken into consideration (Royal Decree implementing the Act of 10 July 2006 on threats, *Belgian Monitor*, 1 December 2006).

Electronic administration – automation of the judicial system
As a follow-up to the Act of 10 August 2005 on the automation of the judicial system (cf. 2005 Report), two acts were adopted. The first introduces electronic legal procedures (the creation of electronic files for both civil and criminal procedures, electronic service, notification and registration procedures). The second modifies certain provisions of the Judicial Code with a view to electronic procedures. The legislator was guided by the principle of necessity (only the provisions requiring amendment have been modified) and of technological neutrality. New concepts have been introduced, such as the electronic legal address, alongside the notion of domicile and residence. A new player will intervene as intermediary among the 'classic' players in the legal world (magistrates, lawyers, public notaries) and the justiciables: the provider of communication services (Act of 10 July 2006 on electronic procedures, *Belgian Monitor*, 7 September 2006 and the Act of 5 of August 2006 amending certain provisions regarding electronic procedures, *Belgian Monitor*, *7 September 2006*).

Electronic administration – automation of the healthcare sector
A health information system (*Gezondheid Informatie Systeem* – GIS) has been set up

in the Flemish community. This system has a dual purpose. On one hand, there will be optimisation of the exchange of data necessary in order to ensure the continuity and quality of healthcare delivery, involving healthcare providers, organisations working in the field and information fora. Within this framework, an individual electronic file for each healthcare beneficiary has been created and is maintained under the responsibility of the healthcare provider. On the other hand, provision is made for optimisation of data exchange with the administration. This refers to the data necessary in order to establish and assess healthcare policy and to amend such policy. The decree also establishes a supervisory commission in the community – separate from the Commission on Privacy Protection, which is a federal body – charged particularly with monitoring respect for the decree, with expressing opinions and recommendations, and with handling complaints and requests for further processing (Decree of the Flemish Community of 16 June 2006 relative to the health information system, *Belgian Monitor*, 7 December 2006).

At the federal level, a draft bill proposing the setting up of a sectoral social security and health committee should be adopted in early 2007 (cf. infra).

B. Jurisprudence

A decision taken by the Termonde Court of the First Instance is evidence of the urgent need for legislation on video surveillance (cf. infra). After an individual had installed several cameras on a public street in order to keep his property under surveillance, it was judged that, irrespective of the fact that the cameras inevitably filmed neighbouring buildings and generally whatever occurred on the street, the Act on Privacy not did apply (*Rechtbank van Eerste Aanleg te Dendermonde*, 25 October 2006).

C. Various major issues

General introduction

The trend to centralise and interconnect data, already noted in recent years, was confirmed in 2006. In its opinions rendered during this year, the Belgian Committee has, as was the case in 2005, focused on the necessary respect for the principle of compatibility among files, in order to avoid the systematic crossing of data, and on the transparency of this processing to citizens. The increase in the number of electronic administration projects (cf. public sector) provided the opportunity for the Commission to reaffirm these principles.

The security objective, both in the sense of public security and financial or commercial security, was addressed in numerous Belgian and foreign initiatives (cf. blacklists and video surveillance). The particular issues surrounding whistle blowing and SWIFT, which the Commission dealt with in 2006, are emblematic of the difficulty in reconciling European protection systems – including Belgian regulations – with American legislation or injunctions with extra-territorial effect.

Police and security sector

<u>*Information services*</u> – On 18 October 2006, the Commission expressed an opinion on a draft bill intended to regulate all data-collection methods used by information and security services. The draft bill provides, in addition to ordinary data-collection methods, for specific methods (such as call-data tracking, identification of the sender of an e-mail, identification of a subscriber, etc.) and exceptional methods (gaining knowledge

of the contents of an e-mail or electronic communication, data collection regarding bank accounts, etc). In its opinion, the Commission first of all points out, with satisfaction, the willingness of the government to establish a legal basis for data-collection methods. At the conclusion of its examination of respect for Article 8 of the European Convention on Protection of Human Rights and Freedoms and for the jurisprudence of the European Court of Human Rights, it points out that there are, however, various problems concerning the requirements for accessibility transparency as provided by the regulation proposed, specifically with regard to the multitude of authorisation and monitoring mechanisms as well as to supervisory bodies. It draws particular attention to the following points:

- the independence and composition of authorisation and supervisory bodies;
- the correct attribution of responsibilities;
- the expertise of whoever is charged with authorisation;
- the balance between the various interests, rights and freedoms at issue.

Video-surveillance – In 2006, the issue of video surveillance was of central concern to both the legislator and the Commission. Several draft bills and bill proposals aimed at creating a framework for video surveillance were submitted to Parliament. The Commission examined one of them in particular. At the end of its analysis, the Commission reaffirmed that, with a view to the principle of legality, the essential elements of video surveillance must be specifically defined by the legislator. The Commission also requested that respect for the prohibition on the recording of sensitive data be particularly monitored by the Commission itself. It also pointed out various serious differences with respect both to the Act on Privacy and European Directive 95/46/EC. As a follow-up to this opinion, the Commission was kept informed of amendments made to this text. Parliament is currently discussing the issue.

The Commission was also asked to express an opinion as to the extent to which an initiative taken by a private day-care centre was compatible with the Act on Privacy. The centre, for children up to three years of age, proposed to install a video-surveillance system (webcams) in the reception area for the children. The purpose of this installation was to enable parents to observe their children on the Internet at specific times of the day. The Commission concluded that the installation was not permissible, out of respect for the children's privacy, and the protection of their data and that of employees, particular consideration being given to the risk of loss of control of the images and hence of their illegitimate reuse.

Public sector

Requests for authorisation for transfer of data flows submitted to the Belgian Commission also show that, in pursuit of administrative simplification – but also, on occasion, as part of monitoring processes – various administrations increasingly intend to couple the data of a given citizen. This is the case, for example, with the data relative to the financial situation of the person concerned for the attribution of rights or advantages subject to income conditions. In these cases, the Commission draws attention to due respect for the principles of legality and purpose, as well as to the right of the person concerned to be properly informed.

Within the context of the preparation of the ambitious project to automate the judicial system (cf. supra), the Commission was asked to examine the possibility of requiring officers of

the court (lawyers, bailiffs, notaries public, etc) to use their electronic identity cards in order to both access Phoenix and to sign electronically any document communicated or registered electronically during legal procedures. Faithful to its jurisprudence, the Commission requires that technical measures be set in place so that a specific, sectoral identification number, different from the national registry number, be used for justiciables, in order to particularly avoid any searching or interconnection on the basis of national registry numbers. It also recommends that the legislator be allowed to intervene in order to specify on the procedures for the use of electronic identity cards by sector professionals.

Private sector

Blacklists – The 2005 Report indicated that the Commission had, at the request of the government, developed principles to provide a framework for blacklists (negative lists). The Commission was of the opinion that it is necessary to legislate in the area of private sector blacklists in order to ensure stronger protection. It also emphasised the need for recourse to a process of prior authorisation for so-called 'sensitive' lists, to additional general guarantees and to internal supervisory mechanisms. In 2006, the Commission was asked to examine a draft bill relative to a framework for such lists. It particularly reaffirms the need to express the illegality in principle of blacklists, except in cases provided by or in virtue of the law. It also invites the legislator to define the conditions that must be met before mentioning persons concerned with external blacklists – the data that must be mentioned are the description of the purpose, the retention period and the procedures for data distribution and access. This regulatory project is still under discussion.

SWIFT – The processing of personal data by the SWIFT company and, in particular, transmission of that data to the United States, where it is examined by the US Treasury in the declared purpose of fighting terrorism, were the subject of two opinions expressed by the Commission. The first examines the compatibility of this processing with the Act on Privacy. The Commission concluded that several provisions – criminally sanctioned – were violated by the Belgian company responsible for the processing. More particularly, the Commission was of the view that SWIFT had committed a serious error of evaluation when it put under surveillance, for several years, a massive quantity of personal data, secretly and systematically, without clear or sufficient justification and without independent supervision in compliance with Belgian and European law. The second opinion was in response to a request from the Belgian Government to specify the substance – from the point of view of data protection – of an agreement with the United States and the form that such an agreement could take. The Commission pointed out first of all that SWIFT was, in any case, required to comply with Belgian and European regulations. As to a specific agreement with the United States, the Commission considers that this is not the only way to remedy the absence of an equivalent level of protection between the legal systems of the European Union and the United States. The Commission prioritises the adaptation of agreements already concluded and existing procedures concerning the fight against terrorism, in compliance with European principles on protection in force, with the recommendations of the Financial Action Task Force (GAFI) and with procedures for the exchange of personal data by means of national financial information databanks.

Similarly, the Commission suggests that the field of application of the framework decision of the Council, relative to the protection of personal data processed within the context of police and legal co-operation in criminal matters, could be amended so as to cover the transfer of private data, as carried out by SWIFT and public bodies such as the US Treasury.

The Commission is closely following the developments in this issue and the measures taken by SWIFT to re-establish activity that complies with Belgian regulations on data protection. This follow-up is carried out in concert with European counterparts represented within the Article 29 Working Party.

Whistle blowing – The 2005 Report pointed out that the Commission regularly received questions and requests for information relative to the introduction of professional guidelines within enterprises (whistle blowing). It then adopted a *Recommendation relative to the compatibility of professional alert systems with the Act on Privacy*. First of all, this recommendation specifies that the setting up of an alert system requires balance, in which the legitimate interests of all players (the organisation, its personnel, the whistleblower, the person in question and any third parties) must be reconciled. The Commission insists on respect for the principles of loyalty, legality, purpose, proportionality and transparency, at both the individual and collective levels. It also considers the rights of the person, those of the whistleblower, the person in question and any third parties, to be paramount.

Security obligation

The Commission adopted Reference security measures applicable to all processing of personal data. Ten fields of action relative to information security have been identified for which any person that stores, processes or communicates personal data must adopt appropriate measures.

Republic of Cyprus

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

During 2006 there were no amendments of the Law implementing Directive 95/46/EC, i.e. the Processing of Personal Data (Protection of the Individual) Law 2001.

In 2006, in co-operation with the Office of the Commissioner of Telecommunications and Postal Regulation, a bill was prepared for the amendment of certain articles of Law 114(I)/2004 (which transposed *inter alia* Directive 2002/58/EC) so that they are fully in line with the Directive. The main amendment related to the transposition into the national legislation of Article 16 of the Directive concerning transitional provisions.

B. Major case law

None to report.

C. Major specific issues

Insurance companies providing private medical insurance

Quite a number of complaints were submitted to our Office by insured persons who claimed that, in order to be compensated for or paid the expenses they incurred for medical examinations, they had to give the insurance company the results of the examination. This was done so that the companies would ascertain that the insured did really carry out the examination and they were not trying to defraud them.

At a meeting with representatives of the insurance companies association we explained our position that this practice, if carried out in all cases without the existence of any indication of suspicion of fraud, was prima facie contrary to the law and should be discontinued.

The installation and operation in public places of cameras which record certain traffic violations

A law which was enacted in 2001 provided for the possibility of recording certain traffic violations though the use of cameras.

In 2006 the system was put into operation, initially for a trial period. Questions were asked in the appropriate parliamentary committee about people having access to the system as well as the period of retention of the relevant data, which mainly concerned the pictures taken by the cameras.

After consultations with our office, the Deputy Chief Police, who is the controller of the system, proceeded to make the necessary arrangements for both issues, which we considered were satisfactory.

The only complaint we have had so far related to the exercise of right of access, to which a solution was found which satisfied the complainant.

Elections for the Greek Orthodox Archbishop

After consultations with our Office, the Electoral Service of the Republic, which keeps the Electoral Register, gave a part of the register that included only the Greek orthodox voters to the Church, which was to be used for the election of the Archbishop. Before that, these voters were given the right to ask that their names be struck off the register before it was given to the Church.

The Electoral Register by law contains the religion of voters as the Cypriot Constitution recognises religious groups who have the right to elect their own representative to the Parliament.

Czech Republic

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

The basic legal regulation in the area of personal data protection is Act No. 101/2000 Coll. on the protection of personal data and amendments to some related acts, which entered into effect on 1 June 2000. The Office for Personal Data Protection (OPDP) was established on the basis of the provisions of this Act and is endowed with all the necessary powers, including direct imposition of fines. This Act essentially implemented Directive 95/46/EC into the Czech legal order. With effect from 26 July 2004, Act No. 101/2000 Coll. was amended by Act No. 439/2004 Coll. and was thus brought into accordance with the aforementioned Directive.

In 2004, the year of accession of the Czech Republic to the EU, implementation of Directive 2002/58/EC was only partly successful. Act No. 480/2004 Coll., on certain information society services which came into force on 7 September 2004, includes particular provisions for unsolicited communications. This Act assigned to the OPDP new strong competences in combating unsolicited commercial communications, including the power to impose severe punishment in cases of breach of the law. Directive 2002/58/EC was essentially subsequently implemented by the Act No. 127/2005 Coll. on electronic communications, which came into effect on 1 May 2005. This Act simultaneously implements a number of other directives belonging to the 'telecommunications package'. The difficult legislative process of transposition of Directive 2002/58/EC into the national law led to some minor imperfections in Article 7 of Act No. 480/2004 Coll., which have been criticised by the European Commission. These imperfections were remedied by expeditious amendment with legal force from 1 August 2006, which also included an important change in the provision of utilising electronic contact data obtained in connection with the sale of products or services for propagation of commercial communications on one's own similar products or services. The original strict rules were replaced by less restrictive legislation based on the opt-out principle.

B. Major case law

In accordance with the Legislative Rules of the Government of the Czech Republic, the OPDP is the mandatory point to which the drafts of relevant Acts and other regulations for observation within the framework of inter-ministerial proceedings are submitted, prior to submitting the draft to Parliament. In 2006, OPDP expressed its opinions on a number of legal regulations and its opinion was respected in most cases. A very favourable effect in implementing the principles of personal data protection during the legislative process is expected from the work of the new parliamentary body – the Standing Commission for Protection of Privacy – which was established in November 2006 in the Senate.

The OPDP competence was specifically aligned or extended during 2006 on the basis of new legal regulations of a sectoral nature. According to the amendment to Act No. 329/1999 Coll. on travel documents and on the amendment to Act No. 283/1991 Coll. on the police of the Czech Republic, both coming in to legal force from 1 September 2006, the OPDP is the competent authority in the first instance on procedures of misdemeanours and administrative wrongs consisting of the illegal processing of data in

data carriers with biometric data. Coming in to legal force from 1 January 2007, the new legal regulation for conditions related to the limitation of some activities of public functionaries and the incompatibility of the position of public functionary with other positions will be applied. These provisions are contained in Act No. 159/2006 Coll. on conflict of interests, which constitutes a new area of personal data processing and, among other things, also stipulates the punishment for misdemeanours processed by the OPDP, consisting of improper management of information from the register of notifications submitted by public functionaries on their activities, notification of property and notification of income, gifts and commitments.

However, it is not always possible to take into account the position presented by the OPDP during the legislation process in passing specific laws, mostly of a sectoral nature. This entails the danger of exemptions from implementation of the principles of personal data protection, because specific laws are employed preferentially over the general law on personal data protection – No. 101/2000 Coll. (Data Protection Act No. 101/2000 Coll.).

For example, Act No. 348/2005 Coll., on radio and television fees and the amendment of some other acts, was first implemented in 2006. In its framework, new conditions were established for collecting radio and television fees, including the manner of keeping records of those who have paid. Although during discussions on the draft law in the Chamber of Deputies the office pointed out inadequacies in this legislation, which constitute a gross infringement of protection of the private legal relation of a citizen to his property, this legal regulation allows processing detailed information on specific data on real estate owned by the payer and his family or persons living with him/her in a common household for the purposes of collection and payment of fees for receiving radio or television broadcasting. The operator of public radio and television broadcasting is authorised to obtain this data from the suppliers delivering electricity to customers.

Another example, where legislation has been adopted which violates the rights to privacy and to personal data protection, is in the manner of discussing and approving amendments to the act on criminal court proceedings and on the police, related to conditions for processing genetic data for the purpose of investigating and preventing criminal activities. This year, at the instigation of the Minister of Interior and without proper analysis of the true state of affairs, the Government and then the Parliament discussed and approved an amendment to the law that extends the police's authorisation to collect and subsequently process biological material, e.g. genetic information, an individual's DNA. According to the new wording of Section 42e (1) of Act No. 283/1991 Coll., on the police of the Czech Republic, "A policeman who, in performing the tasks of the police, cannot obtain personal information permitting further identification in any other manner shall be authorised for persons accused of an offence, for persons punished by imprisonment for an intentional offence, for persons on whom has been imposed protective treatment, or persons who have been found, for whom a search has been declared and that do not have full legal capacity, not only to take fingerprints, determine physical characteristics, perform measurement of the body, take visual, audial and similar records, but particularly to take biological samples permitting obtaining of genetic information."

The third example of problematic legislation consists of the discussion on the draft Act to amend Act No. 266/2994 Coll. on railways. In one of the final stages of its approval in the Czech Parliament, without consulting the OPDP and without any opinion from any of the relevant ministries, it was proposed that private entities (carriers) be allowed access to the registers intended for use by the public administration – the information system on inhabitants – for the purpose of determining the true identity of non-paying passengers and lost fares.

C. Major specific issues

Control activities performed by the OPDP in 2006 included mainly ad hoc controls, i.e. examining complaints. A total of 154 such controls were performed and 90 were completed – these figures do not include controls concerned with unsolicited commercial communications (spam). In addition, 14 inspections were based on the annual plan of control events, which concentrated on 5 general areas in which serious problems had been identified on the basis of negative experience in the past, i.e.:

- information systems of public administration (especially the sectors of finance and the interior);
- chain stores (especially supermarkets, from the viewpoint of clients and employees);
- the system of monitoring people, especially camera systems;
- processing of birth identification numbers;
- electronic communications.

The mass ***introduction of camera systems*** is especially alarming.

Under certain circumstances, operating a camera system can constitute personal data processing in the sense of the law and thus data controllers have, amongst other things, the obligation to notify OPDP of this so that the processing can be registered. In 2006, approximately 350 controllers operating camera systems requested registration, which is a substantial increase compared to previous years (about five carriers were registered in 2005). Nonetheless, this is still quite a small fraction compared to the actual number of installed camera systems in the Czech Republic, which are being increasingly installed in schools, museums, residential buildings, banks, chain stores, etc. The OPDP even obtained a number of notifications where the operator of a camera system intended to place the monitoring of a particular area (public areas, stores, Internet coffee shops) online. Data controllers very frequently notify the OPDP through the notification form that they intend to process the personal data of employees through camera monitoring for the purpose of controlling their work at the workplace. In a number of cases, the OPDP refused to register the processing of personal data by a camera system and issued a decision in which it did not permit this processing. In January 2006, the OPDP issued a written position on the subject of camera systems, which also contained the main principles of operating camera systems from the law's viewpoint.

There has been a great increase in the activities of the OPDP concerned with ***unsolicited commercial communications*** (spam). In 2006, the OPDP obtained 1 296 instigations; 163 controls were begun of which 153 were completed. The most frequent cases of violation of the law can be summarised in the following points:

1. Many of the controlled entities referred to consent granted over the telephone and

almost no one consistently respected the *opt-in* principle where the law requires this.

2. Almost no one declared the communication to be a commercial communication. The messages have all sorts of designations – newsletter, information, news, etc. However, the Act on Certain Information Society Services stipulates that a commercial communication must be 'clearly and plainly' designated as such.

3. Some providers of Internet services contribute towards obscuring the interpretation of the legislation in that they do not send out the commercial communications themselves, but insert advertising footnotes at the end of messages they transmit, i.e. short advertising messages placed as a footnote to an e-mail.

4. For some providers of electronic services, demonstrating consent is limited to ticking a box on the registration form in the relevant section of the web application. They neglect the fact that such a form can be filled in by anyone (and thus for anyone) if it is not protected by an access name and password.

5. If commercial communications are to comply completely with the provisions of the law, they must be properly accompanied by a valid address, to which the addressee could directly and effectively send information stating he does not want the sender to continue sending commercial information. However, if the sender has his database of clients organised according to e-mails, a discrepancy occurs if the sending address of the client is different from the registered address.

Extensive activity of the OPDP in the area of international co-operation was concerned with the long-term ***project of assistance to Bosnia and Herzegovina***. Together with the Spanish Data Protection Agency, the OPDP commenced implementation of the project 'Support to the Data Protection Commission of Bosnia and Herzegovina' (BA04-IB-OT-01) on 1 February 2006. The project is funded by the European Union and is being performed in the framework of the CARDS programme for the countries of the Western Balkans. It is the project's general target to support the institution building in Bosnia and Herzegovina as one of the preconditions for successful progress of the stabilisation and association process in this country. Specifically, this means establishing the legislative and administrative platform for personal data protection in Bosnia and Herzegovina. This is to be achieved in three ways:

- modifying the relevant legislation towards the standards usual in the EU;
- proposing a suitable structure and means of functioning for an independent body for supervision in data protection;
- a successive raising of awareness in data protection amongst citizens, enterprises and state institutions.

The 14-month project is being performed under the twinning concept. One expert from the OPDP is working in Sarajevo throughout the duration of the project as a twinning adviser. Further professionals from the OPDP and the Spanish agency, and two external consultants from Italy and the United Kingdom provide their experience at short-term working meetings, conduct workshops on detailed specific subjects and prepare manuals. The project will be completed on 31 March 2007.

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 transposed into national law in Denmark by:

- The Danish Constitution;
- Act on Marketing Practices, Section 6 (cf. Act No. 1389 of 21 December 2005);
- Act No. 429 of 31 May 2000 on Processing of Personal Data;
- Act 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;
- Chapter 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 2006, the Ministry of Justice proposed legislation to aid law enforcement in the fight against terrorism. Among other things, the proposal included extended possibilities for disclosure of data from government bodies to the police intelligence unit, access for the police to ask public and private bodies to install video surveillance and to keep recordings for a certain time period, and an obligation for airlines to process data on passengers and crew in flights to and from Denmark and disclose them to the police intelligence unit – also by giving the police intelligence unit access to the airlines' booking systems.

Regarding disclosure of data from government bodies, the DPA found that such an extended disclosure could not take place based on the rules in the Data Protection Act, but needed separate legislation. Furthermore, the DPA expressed concern that the access to disclosure was too wide, and remarked that a relaxation of the rules concerning disclosure of data in the Act on Processing of Personal Data is only possible if it is not in conflict with the data protection directive. The DPA particularly drew attention to article 13(1).

In connection with the proposals regarding video surveillance, the DPA cited the practice of the DPA, according to which public as well as private bodies should not set up video surveillance in public areas, and according to which data controllers can only process and retain data, for which they themselves

have a need and a purpose. Therefore, public and private bodies cannot process data with the sole purpose of disclosing it to law enforcement authorities.

Regarding the obligation for airlines to process data on passengers and crew, it was the opinion of the DPA that airlines, according to the aforementioned, cannot on the basis of the rules in the Data Protection Act process data solely for the purpose of disclosing them to the police. The DPA expressed the same views in this matter concerning the disclosure from government bodies.

Finally, the DPA remarked that the rules containing the rights of the data subject will apply when airlines collect and process data concerning passengers and crew.

2. In connection with the reform of the Danish municipal system, the government and the tax authorities intend that municipalities will establish a series of citizen service centres. The centres are to be run by municipalities acting as data processors for the tax authorities and as data controllers in other activities.

The DPA had doubts as to whether it is necessary to give the centres nationwide access to the data controlled by the tax authorities, or if the access could be limited to information concerning the citizens within the jurisdiction of the centres. In principle, access for other centres to personal data can only take place with the consent of the data subject, and this should be clearly marked in the electronic file of the data subject. The DPA also demanded that the log of the system be made subject to random checks that access to personal data was legitimate.

The DPA also demanded that the system log of processing controlled by the centres be made subject to random checks. This is the first time the DPA has gone beyond recommending a random check of the log.

B. Major case law

1. The DPA was asked to give an opinion regarding the project 'e-records'. The purpose of the project was to give GPs (doctors) access to the existing electronic patient records of hospitals, with the consent of the patient. The reality of the project was that all doctors in principle were given a technical access to data concerning all patients in Denmark if they knew their national identification number.

The DPA found that such a technical access should only be given to the doctor who is actually treating the patient. The DPA referred to its recent practice, according to which public bodies and their employees should only have access to data needed for them to perform their tasks.

Since it was not currently technically possible to make such a limitation in the system, the DPA accepted that the system was initiated with another solution regarding access to patient data.

According to the alternative solution, the system will check if a person is normally a patient with the doctor accessing their data. If this is the case, the doctor can with the consent of the patient access the data without further warning. If the person is not a regular patient, the doctor is, among other things, informed that data should only be accessed if there is an emergency, and warned that illegal access is penalised.

The DPA demanded that additional security measures be implemented besides the 'usual' measures already provided by the system (encryption, system log, etc.) The participating counties are obliged to check the system log so that they may detect any unusual behaviour or possible unauthorised access.

Patients are to be informed by e-mail or post if a doctor other than their own has gained access to their personal data, and they will be given an online access to information contained in the system log as to who has accessed their data.

Furthermore, as a minimum, 1% of all 'normal' access to the system and 10% of all access in emergency situations must be checked by the data controller to see if the access was legitimate.

Finally, the DPA emphasised that the optimal safeguards would include a limitation of access ensuring that doctors were only given access to data concerning patients actually in their care, and recommended that such a solution be implemented as soon as was technically possible. The DPA suggested that the patient be given a card that gives an electronic verification before the doctor can access the data.

2. The Museum of Danish Resistance requested an opinion from the DPA regarding a database containing members of the Danish resistance under the occupation 1940-1945. The database was to be published on the Internet. It was the opinion of the DPA that information about a person's connection to the resistance is purely private data covered by section 8 of the Act on Processing of Personal Data. The DPA also found that the material could contain sensitive data in the form of criminal convictions or political opinions.

The DPA stated that the publication of personal data regarding living persons can only take place with the explicit consent of the data subject.

Regarding deceased data subjects, the DPA found that publication of information regarding political opinions can only take place if the information has been publicised by the data subject himself when he was alive (section 7(2)(3) of the Data Protection Act) corresponding to article 8(2)(e) of the Directive). The DPA stated that such a publication could have taken place through the media, books or other means, as long as the publication took place on the initiative of the data subject.

The DPA found that sensitive information covered by section 8 of the Data Protection Act, as mentioned above, could not be publicised under the present circumstances. However, the DPA was willing to reconsider the case if the Museum of Danish Resistance after reviewing the matter should decide to make suggestions to clearly and narrowly define the groups of deceased data subjects contained in the publication.

3. The DPA was contacted by Scandinavian Airlines Service (SAS) regarding SAS' intent to process biometric data about their passengers in the form of a fingerprint template. SAS' plan was to scan the fingerprint of the passenger at check-in and again at boarding in order to ensure that the passenger checking in a piece of luggage is also the passenger boarding the flight.

It was the opinion of the DPA that the biometric data – a template or mathematical value of the fingerprint – is covered by section 6 of the Danish Data Protection Act and not the sections concerning sensitive data.

The DPA found that the processing can take place with the explicit consent of the data subject. In this context, the DPA noted that passengers who do not wish to have their fingerprint processed can use an alternative, manual check-in procedure.

The DPA did not find the processing in violation of the principles of proportionality and purpose limitation. This was based on the fact that the fingerprint templates will be processed for just a short amount of time, approximately 20-60 minutes.

C. Major specific issues

1. Through media coverage, the DPA became aware that several matchmaking agencies on the Internet did not comply with the obligation of prior notification in the Danish Data Protection Act.

The DPA decided to run a campaign to inform these data controllers of their obligation to notify the DPA of their data processing and obtain an authorisation from them.

The DPA contacted the matchmaking agencies in question and informed them of their obligation to notify the DPA of the processing, which resulted in notifications from nearly all agencies. Some decided to end the processing after being informed of the rules on the processing of personal data.

2. The organisation of practitioners of alternative healthcare (acupuncture, zone therapy, etc.) contacted the DPA and asked for assistance with informing the organisation's members of the rules regarding processing of personal data and the obligation to notify the DPA of the processing.

Subsequently, the DPA published a guide to notification for practitioners of alternative healthcare on its website, including descriptions of the relevant sections in the Data Protection Act and a step-by-step guide to the application form.

The initiative has so far resulted in approximately 300 notifications.

3. 2006 has, like previous years, brought a great deal of focus from the DPA to the reform of the public sector set to come into force on 1 January 2007.

In 2006, much of the DPA's attention has been directed at finding a practical solution for the many changes regarding notifications and authorisations given to public bodies, counties and municipalities, which are to change data controllers in the reform.

For example, all counties will be closed in favour of five regions and the number of municipalities will be reduced from approximately 270 to 98.

This has involved a large project within the DPA to evaluate and review the notification system in an effort to make it more effective, as well as making all the changes necessary following the vast amount of data controllers who will cease to exist, change their name or take over activities previously administered by another authority.

The new notification system of the DPA will make it even easier to notify the DPA of processing personal data, and will enable the DPA to spend fewer resources on the large amount of notifications coming in on a continual basis.

Estonia

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

During the year 2006 there were no legislative changes in the Personal Data Protection Act (PDPA)[1]. The new version of the PDPA, passed on 15 February and coming into force on 1 January 2008, includes several amendments that are related to an implementation of the Directive 95/46/EC.

Since at the time of its preparation, the PDPA was based upon the European Parliament and Council Directive 95/46/EC regarding individual protection in the processing of personal data and the free movement of such data, the current year's legislation has also primarily preserved the principles of valid legislation, which are specified, if necessary, and harmonised in their wording.

During the last year there have been no legislative developments concerning the Directive 2002/58/EC either.

B. Major case law

During the year 2006 there were several cases involving the Estonian Data Protection Inspectorate which deserved extensive public attention.

The first selected case concerned medical treatment invoices that were found on the highway. The documents found were D-parts of sick-leave certificates for patients who had visited Narva Haigla, a women's clinic. Before 2002, documents containing sensitive personal data in Narva Haigla were destroyed by burning for which, according to available testimony, a contract was concluded with the boiler plant operating in the city's treatment system; however, at the time of the proceedings it was no longer possible to verify the existence of the contract. It is not possible to determine when and by whom the D-parts were actually taken for destruction, since the destruction certificates for the documents were absent. Narva Haigla also failed to control whether the documents containing sensitive personal information, which were sent for destruction, were actually destroyed or not. As a result of this a situation arose where certificates for sick leave containing sensitive personal data became available to everyone.

Narva Haigla offers residents consultation services with general practitioners and medical specialists, during the course of which personal data describing the patients' state of health are processed. According to the Personal Data Protection Act § 4 (3) 3) a person's data describing their state of health is sensitive and the Personal Data Protection Act § 6 (6) must be followed during its processing, pursuant to which the responsible and authorised processor of the data is required to follow the security principles during the processing of personal data. According to the security principles, security measures must be implemented to protect personal data and to prevent their unwanted or unauthorised amendment, their publication or to prevent their destruction. During the misdemeanour proceeding it was discovered that Narva Haigla did not implement the protection of personal data using the required organisational, physical and information technology security methods as prescribed by PDPA § 6 and § 19.

[1] Personal Data Protection Act is available at: http://www.legaltext.ee/et/andmebaas/ava.asp?tyyp=SITE_ALL&ptyyp=I&m=000&query=personal+data+protection+act&nups.x=12&nups.y=14

Pursuant to this, on 6 June 2006, Estonian Data Protection Inspectorate prepared an expedited procedure decision, and Narva Haigla was issued a monetary fine for the amount of 15 000 Estonian kroon.

The second selected case was called 'Issuing of data from the register of persons liable to service in the Defence Forces'. The Estonian Data Protection Inspectorate began a misdemeanour proceeding regarding the matter where a company called Mindworks Industries OÜ had concluded an agreement with the Northern Department of National Defence for development work regarding the register of persons liable to serve in the Defence Forces and for its applications. As a result of this, the private limited company, pursuant to § 8 of the Personal Data Protection Act, acted as an authorised processor of personal data. In June 2005, one of the employees of the authorised processor took with him from the then Northern Department of National Defence, upon completion of his duties, a USB memory stick on which was saved, in unencrypted form, data for 302 067 men.

It involved male citizens born between the years 1950 and 1987, or in other words the data of all persons liable for service in the Republic of Estonia's military. The data contained personal identification codes, first names and surnames, father's names and place of residence. The employee lost the memory stick, along with the data saved on it, in a public park in Tallinn.

The described loss was made possible because Mindworks Industries OÜ did not implement the required organisational, physical or information technology security measures prescribed by the Personal Data Protection Act for the processing of personal data.

This resulted in the violation of PDPA § 19 (1) 3), following which the responsible and authorised processor is required to put into place organisational, physical and information technology security measures regarding the protection of the confidentiality of personal data from unauthorised processing.

Pursuant to subsection 2, clause 6 of the same section the authorised processor is required to ensure that with the forwarding of personal data via data communication equipment and transporting via data mediums, arbitrary reading, copying, amending or deletion does not take place. With reference to PDPA § 19 (2) 7), the responsible and authorised processor is required to design the organisation of work in the company, agency or association in such a manner as to allow for the performance of data protection requirements.

PDPA § 20 (3) requires the responsible and authorised processor to ensure the training of persons working as subordinates in personal data processing.

In May 2006, the Estonian Data Protection Inspectorate prepared a proceeding decision, for which Mindworks Industries OÜ received a fine of 15 000 Estonian kroon for the violation of PDPA § 19 (1) 3), IKS § 19 (2) 6) and 7) as well as PDPA § 20 (3).

C. Major specific issues

The Personal Data Protection Act entered into force on 1 October 2003. The objective of the new act prepared by the Ministry of Justice during the last year was to improve some grey areas which had appeared during the implementation of the law. During the last year

the Estonian Data Protection Inspectorate has been involved with the preparation of a new version of the law.

Officials of the Estonian Data Protection Inspectorate participated in various national workgroups, for example electronic health and infectious disease observation workgroups, e-file, a biometric workgroup, etc. The electronic health system will be for the whole state involving an innovative and intelligent patient-centric system that enables the collecting, saving and processing of health information. It is an information and communication technology that assists and enhances the prevention, diagnosis, treatment, monitoring and management of health. Our officials have been involved as experts of data protection and technological security in this workgroup.

Finland

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

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, and 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 on a matter concerning a violation on the secrecy of electronic communication.

B. Major case law

A person asked an opinion from the Data Protection Ombudsman in the following case. During the job interview the interviewee had noticed that the employer had searched information about him on Google. The information found was a summary of a panel discussion, which was five years old. The employer used this information and made conclusions based on this information.

In Finland there is a special legislation concerning the protection of private life specifically in the area of working life. It relates solely to the relationship between employee and employer. The act applies to employment relationships and the scope of application covers all employment relationships.

The act applies to civil service relationships and to comparable service relationships. The act relates to state, municipal and church officials or to people in the service of independent public institutions. The act on the Protection of Privacy in Working Life (759/2004) includes the general requirements for collecting personal data about employees and the employer's duty to provide information. The supervision of this act is divided between the occupational health and safety authorities and the Data Protection Ombudsman.

According to this act the employer shall collect personal data about the employee primarily from the employee him/herself. In order to collect personal data from elsewhere, the employer must obtain the consent of the employee. However, this consent is not required when an authority discloses information to the employer to enable the latter to fulfil a statutory duty or when the employer acquires personal credit data or information from a criminal record in order to establish the employee's reliability.

According to the Act on the Protection of Privacy in Working Life, the employer shall notify the employee in advance that data on the latter is to be collected in order to establish his/her reliability. If information concerning the employee has been collected from a source other than the employee him/herself, the employer must notify the employee of this information before it is used in making decisions concerning the employee. The employer's duty to provide information and the employee's right to check the personal data concerning him/herself are also subject to other relevant provisions of the law.

The information searched by Google and other comparable services have been criticised on the basis of unreliability of information. The above-mentioned act requires the employer to collect personal data about the employee primarily from the employee him/herself. Therefore the Data Protection Ombudsman considered that the procedure by the employer in this case had been against the Act on the Protection of Privacy in Working Life.

C. Specific issues

The third national information security strategy

The strategy is part of the Government's Information Society Programme and was drawn up, along with other strategy processes, in co-operation with decision-makers and actors from various sectors of society. A total of about 400 specialists from Government, local authorities, higher education institutions, businesses and organisations participated in the process. The third national information strategy was published on 26 September, in connection with the Helsinki ICT Week.

The objective of the new information society strategy is to support the emergence of a 'Finland phenomenon';, in other words, turning Finland into an internationally attractive, humane, and competitively expert and service society. According to its vision, the strategy pursues good life in an information society.

Guidelines and measures aimed at promoting the reform of the service sector, citizens' wellbeing and the nation's and companies' competitiveness will occupy a prominent role in the new national information society strategy. The aforementioned themes will be addressed from various angles: development of skills, application of existing and new data, creativity and innovativeness, structural and functional reforms, networking, and the development and utilisation of ICTs. The proposed main projects for 2007-2011 include:

- the launching of a policy programme to renew service structures within public administration;
- efforts to increase the speed of data network connections and ensure the interoperability of information society structures;

- measures to promote lifelong learning;
- reform of the rules governing working life and development of leadership and management skills;
- reform of the innovation system;
- further development of the copyright system;
- the promotion of the digitalisation of business in SMEs;
- a contribution to international efforts, especially at EU level, and close co-operation with neighbouring regions and Asia.

National Security Day

The office of the Data Protection Ombudsman participated in the launching of the third national data security campaign and data security day in February 2006. The aim of the data security day was to improve citizens' skills in operating in the information society. The national security day was launched together with public administration, private companies and organisations. This time the day was focused primarily on schoolchildren and their teachers and parents, and the project was carried out in the form of educational Internet games.

Ubiquitous computing

Ubiquitous technology enables people to access and share information in various places and situations with the aid of various devices. Encryption devices and application-level security models are important in supporting privacy, but privacy management is at least as important and a difficult problem. Privacy management must be tied to the way people understand and already manage their private information. Users must be made aware of the privacy implications of their actions and learn how they can implement privacy features as a non-intrusive part of applications and services.

The Finnish Ministry of Transport and Communications commissioned a university research institute, the Helsinki Institute of Information Technology, to produce a forecast extending as far as the year 2015. The forecast was drawn up by 15 researchers from the Institute, each representing different fields of academic knowledge. The report sees many good opportunities for accelerating the development and supporting national welfare, but it also sees plenty of quite challenging threats.

Technological research is very important for Finland. In the next three years or so, 25% of employed people will retire. There is a risk that the national economy will have to spend its money on the welfare of its citizens, instead of investing in research and development. This, in turn, might lead to the weakening of Finland's excellent international competitive ability. The answer to this challenge is to make the production of services to the administration of business and industry more efficient by the increased use of information and communication technology.

Finland has relatively good starting points for this. Nonetheless, approximately half of the population is concerned about data security and data protection. Therefore, it is in the best interest of everyone involved to create systems that citizens, business and industry can trust, which are user-friendly and economical. Fortunately, this has increasingly been understood in Finnish society. Data protection has become a success factor for people in all walks of life. It has made its way from the fringes of legal science to play a central role in society.

France

A. Legislation

Numerous legislative and regulatory texts adopted and published in 2006 had a direct impact on the activity of the National Commission for Information Technology and Civil Liberties (CNIL) during the year.

As a case in point, on 23 January 2006, the French Parliament adopted a far-reaching Anti-terrorist Act, which was followed up by new regulatory texts submitted to the CNIL. These texts provide for additional computer applications for surveillance and extend the possibilities for access and use by police services of data originally collected for another purpose. It is important to point out that, since the act establishes various conditions for carrying out this processing, the CNIL's margins of manoeuvre have been significantly reduced.

The Anti-terrorist Act thus provides for the carrying out of automated processing of data collected by air, rail and maritime carriers. Data on passengers travelling to or from countries outside the European Union may now be processed for the purposes of border control, the fight against illegal immigration and the fight against terrorism. The CNIL expressed its opinion on the texts applying these provisions.

The CNIL expressed its opinion on other texts in application of the same act that provides, for reasons related to the prevention and repression of acts of terrorism, for authorised agents of police services and national gendarmeries especially assigned to these missions to access, according to conditions established by the Act of 6 January 1978, the following data:

- the National Registration File (FNI);
- the National Drivers Licence Administration System (SNPC);
- the National Identity Card Administration System (CNI);
- the Passport Administration System (DELPHINE);
- the Computerised System for Administration of the Files of Foreign Nationals in France (AGDREF);
- the Foreign Nationals Visa Issuing System (BIODEV).

Finally, the CNIL examined the draft decree extending the possibilities for use by the police services of data deriving from the use of electronic communication services, and, in particular, enlarging the definition of persons required to hold such data.

In addition, the application decree particularly drew the attention of the CNIL. The decree specifies the legal requirements with respect to electronic data processing carried out by the majority of public bodies or legal persons under private law. On 30 May 2006, the CNIL submitted a very detailed opinion on this text, saying that it did not contain sufficient guarantees, particularly with respect to the list of public and private bodies likely to ask for telematic or computerised information.

In any case, the Commission points out that Article 60-2 of the Code of Criminal Procedure is essentially intended, as shown by the parliamentary proceedings, for telecommunications operators and excludes from the field of electronic requisition the data covered by professional secrecy, which raises questions since the draft decree is intended to apply to, among others, administrations and

social security bodies which administer precisely the data protected by professional secrecy.

Furthermore, a major draft bill relating to the prevention of delinquency was examined by the CNIL in June 2006 and gave rise to various comments, particularly regarding the intervention conditions for social players and municipal authorities in the case of persons in difficulty.

B. Jurisprudence

No major decision was taken in 2006 which influenced the interpretation of the French Act on Data Protection.

However, it may be pointed out that the Criminal Division of the Court of Cassation, in a decision of 14 March 2006, confirmed the sentence of a company manager who had sent numerous advertising e-mails to Internet users whose addresses had been seized in public Internet space. This decision put an end to the litigation arising from the 'spam box' operation initiated by the CNIL in 2002.

In October 2002, subsequent to its 'spam box' operation, the CNIL had reported five companies to the prosecuting attorney which were practising this type of illegal commercial prospecting. Only one of these accusations resulted in a criminal prosecution.

The person responsible for the company in issue was prosecuted for having collected personal data, in this case, electronic addresses, with the objective of setting up files of prospects by using software able to 'suck' these addresses from the Internet (sites, directories, fora), without the persons concerned either having given their consent or having being informed. Article 226-18 of the Criminal Code penalises the collection of personal data through fraudulent, unethical or illicit means.

The Court of Cassation thus approved the interpretation made by both the CNIL and the Court Appeal, which stated that the use of the two software programs by the company in order to 'suck' the electronic addresses of natural persons from the Internet constituted illicit, and in any case fraudulent, collection of personal data.

On another point, the Court of Cassation also validated the position taken by the Court of Appeal and the CNIL, considering that 'the fact of identifying electronic addresses and using them, even without recording them in a file, in order to send their owners electronic messages, constitutes the collection of personal data'.

The Act on Confidence in the Digital Economy (LCEN) makes the use of e-mail for commercial prospecting subject to the prior consent of natural persons. Nevertheless, the decision of the Court of Cassation retains all of its scope for non-commercial communication by means of e-mail. It clearly establishes that electronic addresses and other personal information accessible in public Internet space are not for free use.

C. CNIL: Functioning and activities

1. The adoption of rulings

In 2006, the CNIL was in session 40 times during 25 plenary meetings, 9 restricted committees (sanctions) and 6 deliberative committees. These meetings led to the adoption of 304 rulings, a volume of decisions similar to that of the previous year but which amounts to an increase of 200% over 2004 and 2005.

These rulings concern the opinions expressed by the CNIL in the execution of its tasks of advising and providing expertise on (a) levying fines, (b) simplifying prior checking formalities, and (c) reporting formalities (authorisation or refusal of authorisations, opinions).

a) Advice and expertise

In 2006, the CNIL expressed nine opinions on draft acts and decrees, among which were its opinion on the draft bill on the prevention of delinquency, its opinion on ratification of a treaty on trans-border co-operation with a view to the fight against terrorism, criminality and illegal migration, and its opinion on a draft bill on the fight against terrorism.

It also made two recommendations: one regarding the files of political parties and individuals elected or candidates for elective position within the framework of their political activities[1]; the other regarding GPS devices in vehicles used by employees[2].

b) Fines

Pursuant to the Act of 6 August 2004, which amended the Data Protection Act of 1978, the CNIL has sanctioning powers enabling it to levy fines to the amount of €150 000 (€300 000 in the case of repetition), within the limit of 5% of turnover. Applying these new powers for the first time, the Commission decided, at a meeting of its restricted committee of 28 June, to levy a fine of €45 000 against Crédit Lyonnais.

During 2006, the CNIL levied the following totals:
- 13 fines for a total amount of €168 000, corresponding to fines from €300 to €45 000;
- 7 injunctions to cease or modify the processing of personal data and 94 formal notifications;
- 4 warnings (to 2 telecommunications operators, 1 bank and 1 political party).

c) Simplification of prior checking formalities

In 2006, in continuance of work undertaken during the 2004-2005 period, the CNIL adopted many measures simplifying prior checking formalities in execution of its services. These simplifications concerned, for example, data processing to assist assessment and selection of credit risk ('credit scoring'), monitoring access to and administration of schedules and meal breaks at workplaces by means of handprint recognition, monitoring of access to workplaces by means of a digital fingerprint when the fingerprint is recorded on an individual data-support, and monitoring access to school canteens by means of handprint recognition. These simplifications are systematically accompanied by very precise frameworks. They are not applicable if those responsible for the processing do not respect all of the related conditions set by the CNIL.

d) Reporting formalities

In 2006, the CNIL adopted:
- 17 refusals of authorisation regarding, in particular, the monitoring of employees by means of digital fingerprints, certain uses of social security numbers and data processing based on name consonance;
- 17 opinions on data processing that is sensitive or harmful; for example, to do with mobile electronic surveillance, telematic or computerised requisitions, the data of airline passengers and the National File of Wanted Persons (FPR).

[1] http://www.cnil.fr/index.php?id=2133
[2] http://www.cnil.fr/index.php?id=1999&news[uid]=342&cHash=7845803996

2. Referrals (complaints and requests for indirect access to police/gendarmerie files)
In 2006, the CNIL received 5 167 referrals (3 572 complaints and 1 595 requests for the right to indirect access to police/gendarmerie files).

The activity sectors that, in decreasing order, elicited the greatest number of complaints are: commercial prospecting, banking, employment, telecommunications. The most frequent complaint is an opposition to processing personal data.

The complaints account for two-thirds of the files examined by the CNIL's restricted committee responsible for levying fines. A quarter of the investigations made by the CNIL originate with complaints made by individuals or with reporting through CNIL's website. Finally, it should be pointed out that, subsequent to a complaint by the committee representing Jewish institutions in France, the CNIL decided to report to the prosecuting attorney those responsible for a website distributing a list of public figures presented as being of the Jewish religion.

3. Monitoring
In 2006:
- 127 entities were monitored (+34.73% with respect to 2005);
- 135 on-site investigations were conducted by CNIL delegations (+40%);
- 25% of the monitoring originated with complaints by individuals.

The principal activity sectors monitored in 2006 were: commercial marketing, private detectives (file management, primarily of debtors, data-collection procedures, etc.), the application of Navigo e-ticketing implemented by RATP (the Parisian Metro network), recruitment, local authorities, biometrics in educational institutions, hotels, safe houses, sports clubs, etc. and video-surveillance systems.

Furthermore, within the framework of international co-operation, facts were monitored by means of a European-level questionnaire sent to ten bodies operating in France and proposing complimentary health insurance contracts. Based on the answers submitted to the CNIL, one of the bodies was given formal notification. In addition, with respect to two other bodies, the decision was taken to verify from a technical point of view that the measures described were actually carried out.

Each of the six hosts participating in a test of personal medical files (DMP) was monitored. The observations resulting from these verifications involving public health medical inspectors for the first time since the entering into force of the new provisions of the Act of 6 January 1978, amended on 6 August 2004, and its Decree of application of 20 October 2005, enabled the CNIL to acquire better information regarding the system implemented before expressing its opinion in 2007 on implementation.

4. Declarative formalities
In 2006, the CNIL recorded 72 000 new instances of personal data processing and 1 800 declarations of modification of processing previously declared, for a total of 73 800 files administered during the year. The annual total number of file declarations to the CNIL has tended to stabilise, since reform of the Act on Information Technologies and Civil Liberties in 2004, which made it possible to exempt from all declarative formalities the files which presented no difficulty with respect to data protection, and to dispense with certain declarations when an officer of information technology and freedom

is appointed. These developments have certainly resulted in containing the flow of file declarations but, in reality, they translate into an increase in activity for the CNIL, which, for example, concerned the training of officers or the drafting of exemption standards.

Since 1978, a total of 1 160 000 files have been declared to the CNIL.

5. Major issues in 2006

a) Biometrics gain ground (identity card, national education, casinos, etc.)

The technological trends observed in 2005 were confirmed during 2006. The main trend regards the continued increase in recourse to biometrics. The CNIL thus had to deal with a net increase in the number of requests for authorisation of biometric devices. In 2005, the Commission authorised the use of 34 biometric devices and refused 5 authorisations; in 2006, it issued 351 authorisations and refused 9.

This spectacular increase in the number of files examined by the CNIL is primarily a result of the adoption, in April 2006, of three simplified authorisation procedures relative to biometric devices:

- recognising handprints with the intention of monitoring access to school canteens;
- regarding the recognition of digital fingerprints exclusively recorded on an individual data-support held by the person concerned and intended for monitoring access to workplace premises;
- regarding handprint recognition with the intention of monitoring access to, and administrating, workplace schedules and meal breaks.

Processing that strictly conforms to one of the three framework decisions (unique authorisations) may be carried out subsequent to a simple declaration of conformity. They concern the purposes most often assigned to a biometric device and represent 299 of the 351 authorisations issued by the CNIL in 2006.

b) Recommendation regarding GPS devices in vehicles used by employees

On 16 March 2006, the CNIL adopted a recommendation relative to the use of GPS devices in vehicles used by employees and intended to provide a framework for the development of these devices in respect of the Act on Information Technology and Civil Liberties and of the Labour Code.

The willingness of the CNIL to adopt a recommendation of this kind results from the observation that, while the increasingly frequent use of GPS systems in vehicles based on the processing of information obtained from satellites is likely to improve the services rendered by the enterprises and administrations using them, such use may give rise to deviations that it would be wise to take into prior consideration.

c) CNIL recommendation on political prospecting

Within the context of the elections in 2007 and 2008, the CNIL decided to adopt, on 5 October 2006 and after consultation with the political parties, a recommendation on the protection of personal data during political prospecting.

The Commission thus pointed out that certain files may not under any circumstances be used for the purposes of political prospecting,

such as files held by administrations or local authorities – civil registries, tax and charge files, social assistance files, etc. The electoral list may be communicated to anyone for use in political prospecting. No legal provision prohibits a party or candidate from using the same means of prospecting as those used commercially, such as the renting of files from specialised companies.

Nevertheless, the Commission is of the opinion that the particular sensitivity of political prospecting requires that the persons whose data are used must be informed, clearly and transparently.

Germany

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

The act on the establishment of joint data files of Federal and *Länder* police agencies and intelligence services (joint-data file-Act – Federal Law Gazette (BGBl) I, No. 66 of 30/12/2006, p. 3409 et seq.) facilitates for the first time in German history the combination of datasets stored at the Federal and *Länder* police agencies and intelligence services in a joint anti-terror data file for the fight against international terrorism.

In the light of both constitutional and data protection law concerns arise, in particular with regard to the respect of the obligation to separate police and intelligence services. This mandatory separation limits the co-operation between police and secret services taking into account the respective different tasks and powers of these different agencies. Also the law that entered into force on 11 January 2007, which is a supplement to the Act on combating terrorism adopted in 2002 (Supplementary Act on combating terrorism – Federal Law Gazette I, No. 1 of 10 January 2007, p. 2 et seq.) seems to be problematic from a data protection point of view. It again increases the intelligence services' powers, which were already enlarged in 2002. The Conference of the Federal and *Länder* Data Protection Commissioners has adopted several resolutions on how to guarantee data protection when fighting terrorism.

Act on the facilitation of small and medium-sized enterprises

On 26 August 2006, the First Act on the reduction of bureaucratic obstacles, aimed in particular at small and medium-sized enterprises, entered into force (BGBl. I S. 1970). This act also makes the mandatory appointment of in-house data protection officers less stringent. This means that the obligation to appoint in-house data protection officers becomes obsolete. However, at the same time, the legal means regarding professional secrets were expanded when it comes to appointing external data protection officers, even in areas in which secrecy rules apply.

B. Major case law

Ruling by the Federal Constitutional Court on data screening 2001 – what are the legal consequences?

In its ruling of April 2006, the Federal Constitutional Court criticised the data screening laid down in the Police Act of North-Rhine-Westphalia resulting from the terrorist attacks of 11 September 2001. The legislator is, according to the Court's decision, only allowed to envisage this intervention in case there exists a threshold of a sufficiently concrete danger to high-ranking legally protected interests, such as the continuity or security for the Federation or a federal state, or for a person's life and limb or liberty. Any data screening without such concrete dangers is not admissible under constitutional law.

The ruling has an impact on the way preventive police data screening in the federal states (*Länder*) and the Federation are arranged. Also other preventive police measures with a similar degree of intrusion and range will have to be judged on the principles established by the Federal Constitutional Court and will have to comply with them.

Ruling by the Regional Court of Darmstadt on traffic data retention

According to a ruling by the Regional Court of Darmstadt of 25 January 2006, which has meanwhile become effective, Internet access providers are in principle no longer allowed to store their flat-rate customers' IP addresses.

The Court has based its ruling on section 96 para. 2 of the Telecommunications Act saying that Internet access providers are obliged to erase traffic data in general immediately after the termination of a connection. Any use of these data after the termination of the connection is only allowed for certain purposes which are detailed in the Telecommunications Act, such as for charging and billing.

This ruling should be welcomed, as the principle of a flat rate means that Internet connections are charged in a lump sum. Against the backdrop of this business model, it is absolutely unnecessary to store the respective IP address of a flat-rate customer for billing purposes.

By this ruling, the Court strengthens the Internet users' right to informational self-determination.

Ruling by the Federal Constitutional Court (BVG) on the rights of insured persons (notice of consent on standard forms)

In a decision dated 23 October 2006 (file no.1 BvR 2027/02) concerning the violation of the right of informational self-determination by a general notice of release from the pledge of secrecy in insurance contracts, the Federal Constitutional Court ruled that such a notice on standard forms and being partly very broadly worded considerably impairs the data subject's interest in an effective informational self-protection.

Given the very general terms of such a notice, it is impossible to specify what information could be obtained by which person, and therefore the data subject is deprived of the chance to personally control how his interests in secrecy are respected. This ruling is of great importance beyond the case concerned, as very broadly worded notices of consent constitute the basis for the collection and processing of personal data in many areas and, as a consequence, the data subjects do not have an alternative to accepting such notices.

Ruling by the Federal Constitutional Court of 22 August 2006 on the use of the IMSI-catcher (International Mobile Subscriber Identity) in criminal proceedings (file no: 2BvR 1345/03)

By means of the so-called IMSI-catcher, it is possible to identify the card number, the device number and the location of a ready-to-receive mobile phone. The Federal Constitutional Court found out that data collected by the IMSI-catcher does not intrude into the confidentiality of communications, but into the right of informational self-determination of third parties not concerned. However, during criminal proceedings, this intrusion is based on a legal binding basis (section 100i code of criminal procedure (StPO)) and is, therefore, not considered disproportionate. However, the Federal Constitutional Court has clearly emphasised that when carrying out such measures according to section 100i StPO, the law enforcement authorities must take into account that the basic right of third parties not concerned must not be affected beyond the strictly necessary measure. Furthermore,

in view of the imminent reform of covert investigation measures in connection with criminal proceedings, the Federal Constitutional Court has called on the legislator to observe closely the technical developments and, with regard to the required protection of basic rights, to take corrective actions if necessary.

C. Major specific issues

On 26/27 October 2006, the 72nd Conference of the Federal and *Länder* Data Protection Commissioners called on the business sector to commit to binding rules when using radio frequency identification devices (RFID). If manufacturers and commerce do not come to a decision, it will be up to the legislator to protect consumer rights in the area of RFID technology. In this context it has to be examined critically as to whether it will be possible to renounce a clear labelling of consumer goods. The respect of certain framework conditions, such as transparency, mandatory labelling, possible deactivation, and effective means of blockage have to be guaranteed when using RFIDs. Any covert creation of profiles is unacceptable. Also the Düsseldorf Circle, a union of the high-level national data protection authorities for the non-public sector, has adopted a similar resolution. Furthermore, the circle 'technology' consisting of *Länder* Commissioners and the Federal Commissioner has produced a guidebook dealing with questions related to data protection law in concrete RFID cases.

The use of electronic signature procedures

Electronic signatures secure electronic documents, in particular their authenticity and integrity. In Germany, in many areas, only the qualified electronic signature has been legally granted the same legal status as the personal signature, and the electronic signature is used to prove the authenticity of electronic documents. Authentication procedures are used between computer systems in order to prove the identity of the systems – if necessary also the identity of a user of these systems.

As a general rule, both systems use the asymmetric encryption. Nonetheless, they differ from each other with regard to the contents of their assertion. This has to be taken into account when planning and using them in administrative procedures (e-Government). The Federal Office for Information Security permanently checks and monitors the security, robustness and the validity of the employed signature procedures. Authentication procedures, on the other hand, only provide an assertion concerning the identity of a person or of a system component. For example, these procedures are used for the authentication of a person or an IT system in connection with a communication partner, or for logging into an IT system.

Therefore, the authenticity and integrity of such data must not be charged with the same legal consequences as a qualified electronic signature. The separation of these two areas is vital for the technical development of a procedure and its application and has to be respected above all in the light of data protection law.

School statistics

For some years, the federal states in charge of school and educational policies have been aiming at a uniform system of school statistics. For these purposes, at the federal state level, it is intended to create detailed datasets about all pupils and teachers, thus documenting the

whole of school life. In addition to that, it is envisaged at a later stage to supplement the pupils' dataset with socio-economical data of the family and to include the years spent at nursery school and at university. These data shall be pseudonymised by an identification number and be connected via a Federation-wide database. As to the purpose of collecting such data, the political side maintains rather vaguely that they are necessary for projects in the educational area.

The 72nd Conference of the Federal and *Länder* Data Protection Commissioners, when referring to the legal provisions of the Constitution, explicitly warned in a resolution against the creation of such a comprehensive register making it possible to relate data to persons. Pursuant to German constitutional law, such a total collection is only admissible if it is impossible to achieve the aim by means of less intrusive measures. According to the Conference of the Data Protection Commissioners, the documents necessary for the project can also be obtained on a voluntary basis by academic research based on random checks. At present, in discussions and workshops with representatives of the *Länder* ministries for education, the data protection commissioners are trying to avert the implementation of this concept which is giving rise to doubts from a data protection point of view.

Research project 'photo-police investigation'

At the central station in Mainz, the Federal Criminal Police Office has tested by means of the research project 'photo-police investigation' as to how far modern face recognition systems can support the police in their search for wanted persons.

During this project, facial images (biometric features) of persons participating voluntarily in the test were recorded and stored in a database for later comparison. The biometric systems compared faces of passing pedestrians with those stored as image data. For the evaluation of the measured data, the facial images of recognised people were photographed, stored and subsequently evaluated.

Provided that the error rate is low, the importance of the combined use of video technology and biometrics will increase considerably. As the technology is in principle appropriate for large-scale individual surveillance, the decisive factor is when and for which purposes a possible later live operation will follow. In this context, the right balance between civil liberties and the interest of public security always has to be struck. It must not result in total surveillance. In addition, it still has to be proven whether and in how far this technology is suitable at all for police investigative measures. Up to now, the Federal Criminal Police Office has not yet presented any field report.

Greece

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

Directive 95/46/EC

Directive 95/46/EC has been implemented into national law by Law 2472/97 on the Protection of Individuals with regard to the Processing of Personal Data. The constant technological advancements as well as the experience gained from the eight-year long implementation of the personal data protection legislation rendered necessary the amendment of certain provisions of Law 2472/97. The current amendment (Law 3471/2006) complements the previous ones (Law 2819/2000, Law 2915/2001 and Law 3156/2003). It does not alter the spirit and the aims of the provisions of the amended law, which aims at guaranteeing a high level of protection of personal data and the provision of the necessary guarantees. The maintenance of a high level of protection offered by the country's legislative framework also guarantees conformity with the requirements of the last Constitutional Review (2001) and in particular with the new Article 9A of the Constitution.

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

Directive 2000/58/EC

Directive 2000/58/EC has been implemented into national law by the aforementioned Law 3471/2006 (on the processing of personal data and the protection of privacy in the electronic communications sector and amendment of Law 2472/97). The new law has been introduced as a new legislative text and not as an amendment of Law 2774/1999 (on the protection of personal data in the telecommunications sectors), which is repealed in its entirety for reasons of clarity and avoidance of confusions.

An English version of Law 3471/2006 will soon be available at www.dpa.gr

Main developments

The Hellenic Data Protection Authority (HDPA) was assigned by Law 3471/2006 Article 29 with the powers to carry out independent audits of the national section of the Schengen Information System, pursuant to Article 114, paragraph 1 of the Convention Implementing the Schengen Agreement (Law 2514 /1997), to exercise the duties of the national supervisory authority as laid down in Article 23 of the Europol Convention (Law 2605/1998) and the duties of the national supervisory authority as laid down in Article 17 of the Convention on the use of information technology in the customs sector (Law 2706/1999).

B. Major case law

Decision 52/2006

By decision 52/2006 the HDPA judged that the recording and processing of data related to representatives of legal entities, who were not debtors themselves, in the file of TIRESIAS Bank Information Systems SA was not legal. The HDPA ordered TIRESSIAS SA to delete all relative data within six months.

Decision 68/2006

By decision 68/2006 the HDPA addressed a warning to a bank and a credit card company to

cease the violation of the Data Protection Law by having granted a loan and having issued a credit card without prior agreement, application and prior information of the data subject. In this particular case someone in charge of a shop selling electrical appliances collected personal data in order to exclusively submit on behalf of a customer an application for a loan to a specific banking establishment. His/her personal data were transferred by the above-mentioned person to another bank in order for the other bank to grant a loan and issue a credit card that the claimant had neither asked for nor had been informed about exceeding the purpose of the contract and his/her consent. According to Law 2472/97, the processing of personal data is allowed in principle and to the degree that the data subject has given his/her consent. One of the exemptions stated in the article 5 2a–e of Law 2472/97 allows the processing to be carried out without the data subject's consent when the processing is necessary for the execution of a contract in which the data subject is party or for necessary steps to be taken at the request of the data subject prior to entering into a contract. The promotion of a banking product and the issue of a credit card without prior information of the data subject and without his/her application is illegal. The collection of personal data by enterprises which co-operate with banks and the transfer of the data to the company that issues credit cards is legal to the extent that the processing is necessary for the issue of a credit card following an application for a credit card on behalf of the data subject (Article 5 par. 1 and 2a) and after having duly informed the data subject (Article 11 of Law 2472/97).

Decision 39/2006

The HDPA received a request from the Ministry of Public Order to grant a permit for the extension of the function of the closed circuit television system on the Attica road network, previously used for the security of the Olympic Games, because, it was claimed, its function was necessary for reasons of public interest and specifically for the purpose of traffic management.

The Ministry had also asked for the processing purpose of the personal data that were being received through the system to be extended. The protection of individuals and goods was declared as the secondary purpose of the processing, which included the following:

a) special prevention and investigation of serious criminal acts with reference to the possibility of using the system during gatherings or assemblies;
b) management of serious cases of safety and crises;
c) protection of important people (VIPs) during their transportation;
d) protection of vulnerable targets (public buildings, embassies, etc.), without having specified them in a more precise and specific way;
e) coordination and control of the personnel of the Hellenic police during the exercise of their duties;
f) recording and transmitting of data to the competent police services, public prosecutor and judicial authorities in cases of fatal road accidents and road accidents involving desertion of the victim, as well as in cases of serious, punishable, criminal acts.

By decision 39/2006 the HDPA permitted the extension of the operation of the closed circuit television system installed on the Attica road network only for the purpose of traffic management until 24 May 2007 under the

terms and conditions stated in the decision No. 63/2004 of the Authority.

Decision 33/2006

The Secretariat General of Information – Secretariat General of Communication of the Hellenic Republic asked the HDPA if, on the basis of Law 2472/97 on the Protection of Individuals with regard to the Processing of Personal Data, it could lawfully ask the competent social security agencies to provide data regarding the time during which the journalists who had been working for the Secretariats on an open-ended contract were insured.

The Secretariat General of Information – Secretariat General of Communication intended to collect the above-mentioned crucial data in order to inform those journalists who met all the requirements to receive full pension and compensation on their right to retire, pursuant to Article 8 of Law 3198/1955, as well as on the right of the Secretariats (as the employer) to terminate their contracts, pursuant to the same article.

The HDPA issued decision 33/2006, whereby it judged that it is against Article 4 of Law 2472/1997 for the competent social security agencies to provide to the Secretariat General of Information – Secretariat General of Communication data regarding the total period of insurance of its employees with a view to terminating their contracts. The HDPA also judged that the creation of such a file goes against Article 4 of Law 2472/97. The decision is based on the fact that the creation and operation of such a file aims at the dismissal of employees solely on the grounds of their age, while the proposed purpose of processing goes against the provisions of Directive 2000/78/EC 'for combating discrimination on the grounds of religion or belief, disability, age or sexual orientation as regards employment and occupation' which prohibit discrimination, both direct and indirect, on the grounds of age as regards employment. Directive 2000/78/EC was implemented into national law by Law 3304/2005, which consequently introduced into the Greek rule of law regulations pertaining to international and Community law which have supralegislative force. Therefore the HDPA prohibits the creation and operation of a file with any type of collection and processing of personal data relevant to the determination of the age of the employees, with the view of terminating their contracts, independently of the special legal nature of the said contracts. Such cases are clearly distinguished from those whereby a legal provision expressly stipulates the termination of a contract due to the retirement of the employee as a result of the employee reaching the retirement age limit.

Decision 49/2006

The company HERMES SA, which provides security services, asked the HDPA if the Athens General Hospital (AGH) in the framework of carrying out an international open tender 'for the procurement of security services based on the award criterion of the most advantageous offer' could lawfully ask the tenderers to submit particular data relating to each of the proposed security guards.

Pursuant to Article 4 of Law 2472/1997, the HDPA examined the lawfulness of providing such data in view of the purpose of processing put forward by the AGH, particularly taking into account the provisions of Law 2518/1997 'on the conditions of operation of private security

service providers, duties of their personnel and other provisions' as well as the provisions of Directive 2000/78/EC 'for combating discrimination on the grounds of religion or belief, disability, age or sexual orientation as regards employment and occupation', which was implemented into national law by Law 3304/2005 (see above dec.33/2006). By Decision 49/2006, the HDPA judged that, pursuant to Law 2472/1997, the AGH can lawfully collect and process the personal data of the proposed security guards. However, the HDPA judged that it goes against the provisions of Law 2472/1997 to collect and process the personal data of each of the proposed security guards regarding their age, taking into account the age restriction (from 23 to 40 years of age) that is in place, as well as their high-school leaving certificate and, for each of the proposed male security guards, the certificate indicating their status in terms of their military service. This is based on the fact that the collection and processing of such data lead to unfair discriminations in the areas of employment and occupation.

Decision 40/2006

By decision 40/2006 the HDPA judged that satisfying the right of access of candidates to their examination papers pertaining to an examination held by ASEP (Supreme Council for the Selection of Civil Service Personnel), as well as to any other public service examination, means that the data subject must be provided with photocopies of his/her examination papers in order that he/she is able to check whether the provisions of the law for the lawful processing of the subject's personal data have been kept by the Controller. In principle, it is clear that a full right of access of the data subject to the personal data pertaining to him/her is consolidated by the provisions of Articles 12 and 13 of Directive 95/46/EC, which has been implemented into the national law by Law 2472/1997. However, the right of access to the said data may be rightfully restricted according to the terms and conditions imposed by Article 13 of the said directive. Such reasons did not exist in this particular case. Therefore all allegations by ASEP in favour of the contrary were unfounded and thus rejected. Directive 2003/98/EC on the further use of information of the public sector has been implemented into the national law by Law 3448/2006. The provisions of the said law neither contradict those of Law 2472/97 nor limit the duties of the Data Protection Authority contrary to what ASEP alleges. Therefore, the Data Protection Authority is fully competent to implement the aforementioned Law 3448/2006. Furthermore, a candidate can exercise his/her right of access any time within the period that the data subject is entitled to claim compensation due to wrongdoing by bodies of the public sector.

Decision 66/2006

By decision 66/2006 the HDPA judged that the provision of Article 22 par. 1 of Law 3475/2006, by which the right of access is denied to candidates of national level examinations for the admission to universities or other institutes of higher education to their examination papers is contrary to the provisions of Articles 12 and 13 of Directive 95/46/EC, that has been implemented into the national law by Law 2472/1997, as well as to the corresponding provisions of the above law. Furthermore, it is also contrary to Articles 2 par 1, 5 par. 1, 9A, 10, 25, 26, 28, 101A, 120, 4 and 20 of the Constitution. Therefore, the Ministry of National Education and Religious Affairs must give access

to candidates to their examination papers and provide them with copies of the papers so that the data subjects will be able to check whether the terms and conditions of lawful processing of their personal data have been kept. The candidates may exercise their right of access at any time within the period specified by the crucial provisions as being the necessary duration for storing these examination papers.

C. Major specific issues

The HDPA is currently developing its new information system, which besides enhancing back office functionality for internal users, it will also provide a new portal offering e-government services to citizens. The e-government services include, among other functions, online submission of complaints, questions and data processing notifications, electronic register of data controllers and advanced search facilities for data protection issues. Citizens and controllers will be able to follow online the progress of their cases. The new information system is expected to be completed by the middle of 2007. In addition, the HDPA has acquired a new switchboard, which especially aids its helpdesk duties. Finally, the HDPA's information system was connected with the national governmental network, SIZEFXIS.

Hungary

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

Directive 95/46/EC

There is nothing to report.

Directive 2002/58/EC

The Directive adopted on 15 March 2006 in the scope of European initiatives referring to the fight against terrorism and organised crime aims to harmonise obligations of service providers regarding the retention of specific traffic data, and to ensure that these data are available for the investigation, detection and prosecution of serious crimes specified by the national laws of the Member States. The Directive however relates only to traffic and location data generated or processed as a consequence of a communication or communication service, and not to data that constitute the content of communicated information. The data retention period may extend from six months to two years, at which point the data have to be deleted.

Regarding other provisions of the Directive, a draft ministerial decree on European Uniform Number '112' has been prepared for providing the legislative background for complying with technical requirements. The amendment of the act on electronic communications for harmonising the Directive was started this year. This act is to give the proper legislative and authorising ground for the aforementioned decree.

B. Major case law

Since the amendment of the Act LXIII of 1992 on the protection of personal data and public access to data of public interest in 2004, the Data Protection Commissioner has the power to make obligatory decisions, against which the data controller may turn to the court. An investigation was started in 2004 which covered data processing issues of a programme on the Hungarian TV channel, RTL Klub, in which two mothers swapped places within their families. Under the contract concluded between the data subjects and the TV channel the illegality of data processing could have been established since the legality of the consent given to the data transmission to unnamed sub-contractors and without temporal and spatial limitation may be excluded. Personal data of minors were also processed for the performance of the contract; however the consent of the parents as legal representatives cannot be acceptable in this regard. The television was called to stop the illegal processing of data. The television brought an action against the Commissioner for changing his opinion. The Data Protection Act opens the judicial way against the decision aiming the termination of the data processing. Such a decision was not made. The Municipal Court agreed with this argument and terminated the action.

Another court case was started by the Hungarian Scientologist Church against the Commissioner. A recommendation was published for the Scientologist Church in which it was called to pay attention to complying with data protection requirements, in particular providing adequate information to data subjects during their religious activities. The recommendation also referred to the expert

opinion of the criminal department of the National Detection Office which had been prepared in connection with the application / applicability of an 'e-meter' as a lie detector by the Church. The Church requested the Commissioner to provide this opinion. However, since the investigation was not finished by the Commissioner, he did not disclose the document. The court action was started by the Scientologist Church referring to freedom of information-related provisions, in particular the disclosure of data of public interest. The action was later repelled because the opinion was delivered to the Church during the action, and the cause of action was lacking.

C. Major specific issues

Civil commotions due to the political crisis in Hungary and related data processing issues raised several problems in October 2006, three of which are mentioned below.

An investigation was started in connection with requests (letters) from the police to hospitals for providing personal data of 'people injured in the course of riots'. The Data Protection Commissioner stated that the letter of the police did not comply with either formal or legal criteria, therefore the data provided by the hospitals would breach the constitutional right of patients to the protection of their personal and special data. In its reply the police named the crime in which its procedure had been initiated and the legal ground for the provision of data and the requested data. It is significant to state that special data may only be processed for specified purposes in relation to criminal procedure. The second letter indicated the purpose as 'processing for criminal procedure', which was too wide a determination. The submission did not comply with the principle of data minimum. The indicated time interval was too long and the type of patient was not specified so that data of patients with no connection to crimes could have been passed to the police. The Commissioner informed the hospital managers that the third and final version of the letter from the police was adequate.

Another investigation also covered the data processing of the police, which was based on notifications that data subjects did not receive regarding their request for information on the recordings of cameras operated by the police and certain other penal institutions. The inspection of the data subjects was also refused after having argued that cameras were not operating in the institutions concerned. The data subjects had intended to use the recordings for procedures to be started against the police – under their right to informational self-determination. Neither party was successful in proving their arguments during the investigation because the legislation related to surveillance systems has too many loopholes. An investigation is to be started *ex officio* in 2007 which aims at examining the applicability and the legal background in Hungary of surveillance systems.

A large amount of publicity surrounded the case regarding data included on the website www.kuruc.info. The names, addresses, home and mobile telephone numbers of judges and prosecutors were published on this site. The names, positions, and workplaces of judges and prosecutors are public knowledge, but the other data are, however, deemed to be personal. Therefore their publication – with the lack of legal authorisation – would have been legal if

consent had been given by the data subjects. It would not have changed the fact of illegality if the data was publicly available – for example in a phone directory or on a website of an animal protection organisation. In the latter case, the data are not related to their activities as judges and prosecutors, and re-publication or other processing thereof is only legal for the purpose consistent or identical with the original intention. The purpose of the data processing of the website is clearly different from this, therefore the disclosure of data in this form was illegal. A further problem was incurred when it was found that the website was not operated on a Hungarian server, and information provided in the imprint was false.

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 having a significant bearing on data protection during 2006.

B. Major case law

The Commissioner issued an enforcement notice against a medical facility that failed to comply with an access request regarding the medical data of a child. The medical facility appealed to Court against the requirement specified in the Enforcement Notice. The appeal was listed for hearing in December 2006. At the Court hearing, the medical facility withdrew the appeal and agreed to supply the personal data sought.

The Commissioner made a number of individual decisions on complaints made under the terms of the Data Protection Acts which were not appealed to the courts. The most significant were:

- A renowned Irish entertainer complained to the Commissioner about publication by a newspaper of a photograph of her with her child together with observations about their interaction. The data subject considered that the data was not fairly obtained or processed. The primary issue to be decided in this case was whether the journalistic/freedom of expression exemption provided for in Article 9 of Directive 95/46/EC (as transposed under Section 22A of the Irish Acts) applied in respect of the publication of the photograph and text relating to the data subject and her daughter. In arriving at his decision the Commissioner took account of Articles 8 and 10 of the European Convention on Human Rights (ECHR) (the right to respect for a person's private and family life and the right to freedom of expression); guidance from the European Court of Human Rights on how these rights should be balanced; relevant codes of practice; and previous decisions from this office emphasising the importance of parental consent and the protection of minors in the context of publication of photos of young people. In his decision on the case the Commissioner found that publication of the photograph and text relating to the data subject and her daughter, and the manner of their interaction, could not be justified in terms of the public interest and that the personal data relating to the data subject and her daughter was not obtained or processed fairly.

- A data subject who received an unsolicited direct marketing message from a telecommunications company complained to the Commissioner about the manner in which his cell-phone number had been obtained. Fans at a music concert were encouraged to text support for anti-poverty efforts. Their cell-phone numbers were stored on a database later used for direct marketing purposes. The Commissioner decided that, because the data had been collected for one specific purpose and used for another, it constituted a breach of data protection legislation. When the telecommunications company initially refused to delete the database, the Commissioner issued an enforcement notice that compelled them to comply.

C. Major Specific Issues

Mortgage Brokers

A media report drew the Commissioner's attention to a number of serious allegations concerning alleged data protection breaches between mortgage intermediaries and estate agents. The allegations centred on the disclosure by mortgage intermediaries to auctioneers of sensitive personal data such as annual income, parental financial assistance, investments etc. The Commissioner gathered the mortgage broker representative bodies together with the financial regulator to discuss the issues involved and remedial actions. The Commissioner also arranged a number of random, on-the-spot inspections of mortgage brokers and estate agents. In the course of these inspections the Commissioner observed a lack of knowledge amongst mortgage intermediaries in relation to the full extent of their responsibilities under the Acts. Following the inspections the Commissioner issued a guidance note and a Data Controller's booklet to all 1,633 mortgage intermediaries registered with the Financial Regulator. The note drew attention to the importance of using and disclosing personal client data in a way compatible with the purpose for which it was initially given. This ongoing engagement and interaction with the mortgage sector has lead to many positive revisions of procedures and codes in relation to customer confidentiality. The programme of random inspections of mortgage intermediaries will nevertheless continue throughout 2007.

Italy

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

- Act No. 38/2006 set up the National Centre for the Fight against Child Pornography on the Internet. Its tasks consist of collecting, from police forces, reports on sites disseminating materials that are related to the sexual exploitation of children; the Centre is also entrusted with keeping a register of such sites, their managers and the respective payees. The Centre collects the reports lodged by electronic communications providers with regard to contracts with companies and/or entities that disseminate or deal in the said materials. A decree implementing this act was recently issued by the Minister of Communications in agreement with the Minister for Reformation and Innovations, after consulting with the Garante, to set out the technical measures connectivity providers are required to take in order to prevent access to child pornography websites.

- Act No. 281/2006 laid down measures concerning the destruction of materials related to unlawful interception and 'profiling' activities; such materials may not be used in a judicial proceeding and must be kept in a secure place as confidential information under the responsibility of the relevant public prosecutor – pending the decision to be handed down by the judge for pre-trial investigations concerning their destruction. This is aimed at preventing acquisition of the materials in question by unauthorised individuals. The act leaves unprejudiced the Garante's power to establish and prevent the unlawful dissemination of data and/or documents and impose the applicable sanctions, including exercising access/rectification rights by data subjects.

- The 2007 Budget Act (Act No. 296/2006, paragraph 542) authorised an increase in the permanent staff of the Garante in order to allow the Data Protection Authority (DPA) to discharge its institutional tasks better with particular regard to supervisory and control functions. The Garante was empowered to increase its staff by no more than 25% of the total number of staff referred to in the Data Protection Code, in compliance with the apportionments made for the next three years (amounting to €21 846 million in 2007, 21 591 million in 2008, and 21 986 million in 2009).

- **Parliamentary hearings:** The Garante was heard several times by Parliament during 2006 with regard to major issues being debated by the competent parliamentary committees – in particular, technological innovations in the public administration and the impact of those innovations on the protection of privacy, in view of ensuring citizens' trust in their relationships with institutions. Additionally, the Garante contributed to the parliamentary inquiry into telephone wire tapping regarding the issues related to compliance with security measures by judicial authorities and telecom operators as well as with regard to publication of the contents of lawful (i.e. authorised) interceptions. Reference can also be made to the hearing concerning the data protection safeguards the Garante had called for in respect of the new pieces of legislation aimed at countering tax evasion – in particular concerning the interlinking of different databases.

- **Opinions:** Under section 154(4) of the Data Protection Code, the Prime Minister and each Minister are required to consult with the Garante when drafting regulations and administrative instruments that are liable to impact on personal data protection. Within this framework, several opinions were rendered by the Garante in 2006 on major issues such as, in particular, coercive medical examinations in the absence of drug addiction; the electronic interlinking of information systems and automated archives managed by the agencies responsible for migration matters; access to administrative documents; collection and retention of the data included in the national register of the entities authorised to apply medically assisted reproduction techniques; management of telephone subscribers' data in connection with the activities falling within the scope of competence of the Ministry for Home Affairs; and card fraud prevention.

B. Major case law

Use of traffic data for different purposes: The Constitutional Court (Judgment No. 372 of 6 November 2006) ruled that the prohibition against using traffic data for purposes other than the fight against Mafia-type crime and terrorism, upon expiry of the retention period (i.e. 24 months) laid down in Section 132 of the Data Protection Code, is not unconstitutional.

Videophones: According to the Court of Cassation (Judgment No. 10444 of 5 December 2005), taking pictures with a videophone, including at the workplace, without the data subject's consent and/or without the data subject's being aware thereof, is an unlawful interference with private life. In the Court's view, Section 615-bis of the Criminal Code is meant to punish unlawful interferences with another's private life as caused by technical implements that can reproduce the violation of privacy resulting from the disclosure of what is not meant for third parties' unrestrained perusal.

Jurisdiction in data protection cases: In an order dated 10 April 2006 (No. 12980), the Court of Cassation ruled that jurisdiction lies with the court of the data controller's place of residence, thereby overriding the rules that apply to jurisdiction in consumer protection cases (set out in Section 1469-bis, para. 3, no. 19, of the Civil Code) – also in view of claims for damages. The Court emphasised that the protection of data subjects afforded by the Data Protection Code is based on a different rationale compared to the protection of consumers, insofar as the latter are parties to a contractual relationship. This can be accounted for, in the Court's view, by the need to ensure that the Court having jurisdiction in such cases is as close as possible to the place where the data are processed and disseminated.

Employment sector: In a judgment dated 13 September 2006, the Court of Cassation (Employment Matters Division) ruled that a company could lawfully dismiss an employee on account of third parties having connected with the corporate network from the outside via the personal password allocated to that employee.

Access to public records vs. data protection: In a judgment dated 21 February 2006, the Council of State – which is the highest administrative judicial authority – ruled that it was illegitimate for a public administrative agency to decide, allegedly on grounds of data protection, that a participant in a public call for tenders could

access the records related to the said call by only inspecting them, i.e. without making copies thereof.

Regarding the same subject matter, a decision by the Council of State dated 7 June 2006 tackled the balancing between access to public records and data protection in respect of the procedures applying to calls for tenders. In particular, the Council ruled that the right of access to public records was vested in the applicant regardless of the violation that might have been caused to the applicant's rights and/or legitimate interests, since this type of access is aimed at ensuring transparency in public administrative activities.

C. Major specific issues

Law enforcement databases

Databases set up for prevention and security purposes by police bodies were among the most significant areas of activity for the Italian Garante. In particular, the Garante focused on the so-called 'joint police intelligence system' set up at the Public Security Department of the Ministry for Home Affairs. This database was set up pursuant to a statute and is managed jointly by the Italian police bodies.

The size of the database, the nature of the data it contains, and the high number of staff that are lawfully entitled to access it for prevention and/or investigation purposes make it a database of major national interest.

The Garante's action consisted of ordering the Public Security Department to take organisational and technical measures and precautions in order to enhance security levels, also with regard to the interlinking with databases held by public and private entities. The most significant measures in question are summarised below:

- Encryption for certain categories of filing system;
- Authentication and authorisation procedures, requiring strong authentication tools to be implemented – including the possible use of biometrics;
- Security auditing;
- High-integrity, high-reliability access and operational logs (certified logging systems);
- Digital workstations certification with a view to asset management and security;
- Appointing an in-house privacy officer in charge of managing both the IT security features of the database and the relationships with the Italian DPA.

This is the first stage of an investigation started by the Italian authority in view of more in-depth analyses concerning the substance of the measures to be adopted, by having regard also to proportionality, purpose limitation, etc.

Additionally, the Garante requested the processing operations performed by law enforcement authorities to be listed in full in accordance with the requirements set out in the Data Protection Code, so as to actually enable inspections and control over their operation – which is currently the case only with regard to the 'joint police intelligence system'.

Reference should also be made to the inquiries carried out by the Garante in 2006 – which are partly still in progress – with regard to the discreet surveillance alerts entered in the national section of the Schengen Information System (SIS). These inquiries were aimed at verifying, in particular, compliance with the

data protection requirements set out in the Schengen Convention as for data quality and accuracy of the information. The Garante also started investigating the mechanisms deployed for the EURODAC database by taking account of both the lawfulness of the processing and of the adequacy of the security measures to be implemented.

Following a report lodged with the authority, the Garante decided to collect preliminary information in view of assessing, including via on-the-spot inspections, the data processing operations carried out by a special investigation squad of the Carabinieri, which allegedly had set up a database containing genetic information taken from crime scenes – to be used for judicial investigations.

The security measures applying to the processing of personal data by judicial authorities and offices were also addressed by the Garante in 2006, on the basis of a co-operative approach involving the relevant judicial authorities. In order to verify compliance with the applicable security requirements, the Garante decided to carry out on-the-spot investigations in some judicial offices.

Security in telephone and electronic communications

In the past year, the Italian Garante carried out in-depth controls on both the processing of traffic data and some security features related to telephone and electronic communications.

The processing of traffic data has been the subject of ever-increasing interest, partly because of the concerns raised in Italy by media reports on several judicial investigations into the unlawful processing of call data records.

Following a complaint lodged by an Italian citizen on account of the allegedly unlawful disclosure of his call data records, the Garante ordered the main Italian telephone operator to take specific measures and precautions in order to enhance security levels. Such measures were focused in particular on the authorisation systems and auditing capabilities of IT systems, which were partly ineffective in respect of technical staff with privileged access features – such as system administrators and database administrators.

The Garante also started an in-depth investigation into the systems deployed by the main telephone operators so as to get the full picture and set out effective measures – in pursuance of Section 132 of the Data Protection Code – to be complied with in retaining such telephone and electronic traffic data as may only be used for judicial purposes.

Furthermore, the Garante took steps to empower security measures in telephone systems in order to protect the information acquired by telephone operators in performing lawful interception activities and, more generally, in co-operating with law enforcement authorities. In particular, the Garante aimed at ensuring that information could be exchanged between telecom operators and judicial authorities via secure communication channels, or else via channels made secure by the adoption of IT technologies; banned any plain-text transmission via non-secure channels; and required the operators to only use e-mail with qualified digital signature and/or secure web-based services with SSL encryption protocols and strong authentication procedures.

As for the broader issue of security in electronic communications, the Garante initiated

exchanges of views and co-operation actions with the other public authorities and institutions in charge of specific tasks in this area.

Data protection and Internet search engines
The Garante took steps to enable data subjects to exercise their right to rectify the data contained on web pages by updating the information retrieved via Internet search engines – in accordance with the principle whereby everyone has the right to accurate self-representation on the Net, regardless of where the relevant information is posted. To that end, the Garante wrote to Google at the company's headquarters in California, USA - where the search engine servers are based – and called upon the company to devise solutions that could do away with persistence on the Net of obsolete and/or inaccurate personal information even after such information had been amended at the 'source websites' from which the relevant pages were extracted. This initiative was based on the claim lodged by an Italian citizen, who had found that information on a criminal proceeding instituted against her continued to be available via Google's search engine even though she had been acquitted of all the charges; this was due to the many cache copies and the various abstracts produced by the search engine, which provided a distorted image of her situation compared with the correct one shown on the source websites. Although Google already has a mechanism in place that allows a website to delete obsolete links and/or non-existing URLs, this is not sufficient to adequately ensure the so-called 'right to oblivion'. Google Inc. was also invited to post a clearer information notice on **www.google.it** explaining that the controller of the processing carried out by the search engine is the US-based company, and detailing how users can quickly have web pages erased or updated whenever such web pages have been modified at the source websites. A meeting was subsequently held with representatives from Google Inc. at the Garante's premises, and a fruitful dialogue was started.

Formal complaints
Four hundred and thirty-five formal complaints were decided upon in 2006. Most complaints concerned processing operations by banks, financial companies and private credit reference agencies. However, some of the cases addressed in the past year tackled new issues attracting special interest, in particular as regards the following:
Two cases concerned the monitoring of employees in the private sector, in particular for the storage of personal files in a company's computer and the monitoring of Internet browsing. In both cases, the Garante ruled that the processing carried out by the employers was unlawful because the employees had not been informed in advance about the possibility that this type of monitoring would be carried out and also because the processing in question was excessive by having regard to the purposes to be achieved (i.e. ensuring the appropriate performance of job assignments). The Garante emphasised, in particular, that the monitoring could be limited to establishing the existence of 'personal files' in the company's computer, without accessing the relevant contents, and to only verifying the duration of browsing, respectively.

Another interesting complaint was lodged by a lady alleging the unlawful use of her image made by a political party, which had posted bills containing her image on the occasion of an enrolment campaign. The lady had recognised herself in the image in question

and applied to the Garante, which granted her complaint because the processing was found to be in breach of her personal identity. The relevant picture had been taken about 20 years previously on the occasion of a public demonstration and its use was liable to represent the lady's personality in a different light from what corresponded to its current status. The Garante ordered the political party to immediately remove the bills and prohibited any future use of the image on websites, printed materials and/or propaganda materials.

A complaint concerning the sending of advertising e-mails allowed the Garante to reiterate the prohibition against sending such e-mails without the recipient's prior consent – also with regard to the initial contact e-mails. The Garante ordered the company in question to erase the complainant's personal data from its database and stressed that an e-mail address may not be used unrestrictedly merely because it can be found on the Net.

Inspections

The inspection activities by the Garante were enhanced in 2006, partly on the basis of the six-month inspection plans developed by the DPA. Overall, 350 inspection proceedings were carried out. They mostly concerned private entities and were aimed at checking compliance with the main requirements laid down in the data protection legislation. In particular, the Inspection Department focused on the processing of personal data by credit reference agencies; the processing of medical data by pharmaceutical companies and healthcare bodies; the online processing of personal data; and the processing aimed at the provision of goods and services via distance selling mechanisms. In performing such inspections, the Garante can also avail itself of a specialised corps within the Financial Police (Guardia di Finanza), which was entrusted with checking compliance with the requirements concerning notification, information notices, security measures and enforcement of the resolutions adopted by the Garante.

Following the inspections, 159 proceedings were instituted with a view to the imposition of administrative sanctions; in 11 cases criminal information was preferred to judicial authorities. Criminal infringements concerned non-compliance with resolutions adopted by the Garante; failure to take minimum-security measures; and the violation of the prohibition against the remote monitoring of employees. The administrative sanctions imposed are expected to yield minimum revenues amounting in 2006 to about €600 000.

Public sector:

Public Administration

In 2006, the public administration was required to take steps in order to adequately take into account and publicise the safeguards provided for in respect of the processing of sensitive and judicial data. The personal data protection code requires public bodies to issue ad-hoc regulations in order to collect, use and retain such sensitive and judicial data as are indispensable for their institutional activities. The regulations in question must specify and provide the public with information on what data is processed and for what purposes. This requirement applies, in particular, whenever specific guidance is not provided to that effect in the laws that, from time to time, authorise public bodies to discharge certain tasks which entail the processing of sensitive personal data. The obligation in question arises out of Article 8(4)

of Directive 95/46/EC, which – as is well known – only allows processing the data at issue on specific grounds in the substantial public interest and by affording suitable safeguards. The draft regulations submitted by public bodies must be approved by the Garante.

As well as being necessary under the Data Protection Code, drafting the said regulations provided the entire public administrative sector in Italy with a significant opportunity to further modernise its structures, including in terms of the available safeguards and operational transparency. In this manner, the public administration could adjust its organisational and functional framework by also having regard to the respect for fundamental human rights and freedoms – which must be mirrored in all the activities carried out by public administrative bodies.

In assessing compliance with personal data protection legislation in different public sectors, the Garante could appreciate the growing social awareness of the need for protecting the fundamental right to personal data protection better and more specifically – also with regard to areas that had not been expressly taken into account yet.

In order to ensure the appropriate application of the Data Protection Code, and in the light of the forthcoming deadline set in the law (i.e. 28 February 2007), the Garante enhanced its co-operation with regions, local municipalities and universities in order to lay down the relevant draft regulations by also making available model drafts; this co-operation was also afforded to the Prime Minister's office and other public bodies by having regard to the respective institutional functions. In this manner, it was possible to ensure that the drafts submitted for the Garante's approval could be streamlined with the regulatory framework from their initial development; this resulted, in turn, in an increase in the number of favourable opinions, which could establish that the guidance provided in the course of the correspondence between the individual administrative offices and the office of the Garante had already been taken into due consideration.

The comparative evaluation of 92 draft regulations afforded the Garante a wider gamut of inputs to systematically assess the mechanisms deployed by the public administration in processing sensitive personal data.

In particular, a few criticalities were found to be quite common, and in some cases this prevented a favourable opinion from being handed down in respect of the draft regulation submitted; more frequently, a favourable opinion was issued, however several 'conditions' were laid down and this considerably increased the casework for the authority. For instance, there was a tendency by some public administrative authorities to pursue the 'legalisation' either of a set of processing operations that fell outside the scope of the relevant institutional competences or of processing mechanisms that were unquestionably disproportionate compared to the purposes to be achieved.

An especially demanding task consisted of assessing whether processing of the categories of sensitive and judicial data specified in the model drafts was actually indispensable. In many cases it proved necessary accordingly to either eliminate certain categories of sensitive and/or judicial data, or else certain processing operations as set out in those drafts.

Opinions were rendered by the Garante, *inter alia*, on the draft regulations submitted by the Ministry for Home Affairs, the Ministry of Defence, the Ministry of Education, the National Research Council, the Court of Auditors, the Council of State, Regional Administrative Courts, as well as several local authorities and research bodies.

Healthcare
The Garante took steps with regard to a hospital in order to terminate the processing of data carried out by the hospital's Internet website, on which pictures of children affected by common childhood diseases had been posted. This case was found to entail the processing of sensitive data related to children, which may not be disseminated and are afforded enhanced safeguards in order not to jeopardise the development of their personalities. As also set out in the physicians' code of practice, it is prohibited for a healthcare practitioner to disseminate, via the press or other media, information that may allow identifying the data subjects; additionally, healthcare practitioners must ensure that patients may not be recognised whenever clinical and/or observation data concerning individual persons are published in scientific papers.

Holocaust archives
The Garante addressed the issues related to access to the so-called holocaust archives that are kept in Bad Arolsen (Germany). A draft regulation on access was developed during 2006 by representatives from the governments of signatory countries to the 1955 Bonn Agreement (which regulated the establishment and operation of the archive) – including Italy. The Garante had no objections against access to the records on the spot for historical research purposes, subject to the safeguards detailed below. However, duplication of the archives, as requested by some countries, would raise far more complex problems; in the Garante's view, it would require an undertaking by all States (including non-EU countries such as the USA and Israel) to afford at least equivalent safeguards – in particular by having regard to the rules applying in the EU to data transfers to third countries. At all events, the safeguards to be envisaged in connection with the archives are those set out in the European data protection directive as well as in the code of practice developed in Italy with regard to the processing of personal data for historical research purposes.

Private sector:
Profiling: Hotels and loyalty cards
The Garante banned the processing carried out by a major hotel chain, which collected data related to customers' tastes, habits, length of stay, and other items of information in order to know their customers better and anticipate their requests, without providing adequate information notices to them and without the customers' consent to further processing operations (for marketing purposes and/or communications to other companies). The Garante prohibited any use of the data collected in the above manner, and required the hotel chain to reword the information notices, request consent for processing the data with a view to profiling and marketing activities, and lay down specific retention periods. Additionally, administrative sanctions were imposed on account of the inappropriateness of the information notices and the failure to notify the processing to the Garante as required by the law.

In another case, concerning a major retailer, the Garante prohibited the processing of personal data that were collected with a view to issuing

'loyalty cards' to customers and were unlawfully used also for marketing purposes. The Garante ordered that the information notices should be reworded to specify that the purposes sought included profiling and communication of customers' data to a bank. In particular, the Garante prohibited the company from making the issuance of loyalty cards conditional upon the customers' consenting to the processing of their data for marketing and profiling purposes.

Condominiums
The Garante has been receiving complaints and requests for clarification with regard to the processing of data in connection with condominiums ever since it was set up. After issuing specific decisions in the past, all the different items were consolidated in a general decision that was drafted in 2006 following a public consultation – so as to give rise to a veritable 'Vademecum' for condominiums. This decalogue provides guidance on how to comply with data protection rules in the different situations related to life in a condominium (such as, for instance, the prohibition against publicly posting a list of defaulting tenants, or the precautions to be taken in processing sensitive data).

Guidelines applying to the collection and use of personal data by private sector employers
A unified framework of guidelines applying to the processing of employees' personal data was laid down by the Garante in December 2006, also following several requests for information and complaints lodged by employees, trade unions and trade associations.

The main points made in the guidelines concern:
a) the need to only process indispensable personal data (data minimisation principle), which also applies to the arrangements concerning visible badges and similar contrivances;

b) the need to adequately inform employees on the use of their data, their data protection rights, and how to exercise them;

c) the need for the employees' consent prior to disclosing their personal data to third parties (also when posting their personal information on billboards and similar devices);

d) the need to refrain from the blanket use of biometrics, which must be reserved for specific, adequately documented cases (e.g. access by certain employees to high-security or dangerous areas) and requires the Garante's prior checking;

e) the need for taking special precautions in handling employees' sensitive data, which must be kept separate from other non-sensitive information

These general guidelines apply to the private sector and will be followed by additional, more specific instruments addressing, for instance, the use of e-mail services and Internet at the workplace.

Credit reference agencies
Following inspections carried out in respect of credit reference agencies (CRAs, or credit information systems as they are called in Italy), the Garante issued six provisions in which the processing carried out by such CRAs was found to be unlawful. This was related, in particular, to the circumstance that several telephone operators used to carry out checks on customers' creditworthiness and reliability by means of the

information derived from CRAs – at the time of stipulating the relevant contracts. In this manner, the data collected by the CRAs for the purposes of protecting credit and reducing the attending risks were disclosed to entities that were not authorised to access such data. Additionally, the information notices provided to data subjects were found to be incomplete and the security measures were inadequate. In some cases excessive data were processed compared to those required in order to verify timeliness of payments.

In another decision, the Garante addressed the retention period of the so-called 'positive' information, i.e. the data concerning regular payments of instalments and/or the extinguishment of debt. The Garante specified that the maximum retention period may not be in excess of 36 months in these cases.

e-ticketing

A decision adopted by the Garante in October 2006 provided an opportunity for setting out some general principles in respect of e-ticketing services. The decision specifically concerned e-ticketing in Rome and Milan, where integrated transportation systems have been in place for some years. Such systems share several features (e.g. smart cards are used in both cases by subscribers; a centralised database has been set up for management purposes and for the analysis of aggregate data), including the possibility to collect additional data (other than those provided by the subscribers in signing up for the service) via the smart cards. Such additional data are stored on the smart card chip (validation data and a given number of validations), on the validation machines at the entrance stations (chip identification data such as serial number, subscription number and validation data) and in the central database (subscribers' ID data, card chip serial number and validation data from machines). The main guidelines provided, to be possibly adjusted in future and also in the light of technological developments, are the following:

- It is permitted to store validation data (time/place) on the e-ticket (smart card), but only if not excessive (four to five validations are enough for the relevant purposes);

- It is permitted to store data (such as the serial number of the e-ticket) on validation machines, but only temporarily – e.g. for 24 hours to match those data with black lists (stolen cards, expired subscriptions, etc.);

- There should not be any centralised storage of a user's ID data associated with the respective e-ticket data: statistical analysis and service improvement do not require personal information. A limited retention period (72 hours) is acceptable in order to manage malfunctioning / problems; thereafter, the data must be anonymised for the sake of data protection and freedom of movement. This leaves unprejudiced the possibility to store the data centrally for longer periods in identifiable format if this is required on specific grounds (e.g. need for in-depth investigations in a specific case).

Unsolicited telephone services

Following a considerable number of claims, reports and enquiries pointing to the occurrence of repeated violations related to the activation of unsolicited telephone contracts, cards and/or services, the Garante considered it necessary to lay down framework safeguards that could ensure respect for

citizens' fundamental rights and freedoms. Different cases were at stake: mobile phone cards activated on behalf of unwitting data subjects; activation of unsolicited carrier pre-selection; or additional telephone services activated either by one's own provider or by another. The Garante stressed that all the entities involved in processing such data are required to ensure that the data are collected and stored for specific, explicit and legitimate purposes and processed, also thereafter, fairly and lawfully by complying with the provisions contained in the Data Protection Code as well as with any other relevant piece of legislation so related to data processing – including the requirement to identify subscribers to and purchasers of pre-paid mobile phone cards before activating the respective services, i.e. at the time the electronic cards are delivered and/or made available. To that end, suitable procedural mechanisms were recommended.

Codes of practice

Work continued throughout 2006 on the draft code of practice applying to the Internet, with the participation of a large number of representatives from trade associations and the relevant industry sector. The codes of practice applying to other sectors (private detectives and investigations carried out by defence counsel in connection with criminal proceedings) are also under way.

In the light of the importance of this tool, an ad-hoc regulation was published in the Official Journal to clarify the mechanisms whereby the Garante can foster the adoption of codes of practice in sectors of substantial public interest that require specific regulations (e.g. employer-employee relationships and marketing). The regulation also sets out the criteria to be fulfilled in order for a given trade/industry association to be regarded as actually representative of the respective sector.

Media

The Garante issued an interim order to block use of the personal data that served as the basis for a TV programme concerning a drug test performed on 50 MPs without their being aware thereof. The Garante found that medical data had been processed unlawfully in this case, especially by having regard to their collection – irrespective of the dissemination of such data via the TV programme. The persons concerned had not been informed about the explicit purposes of the processing, and their biological samples had been collected in a misleading, unfair manner. Based on these grounds, the Garante prohibited the collection, storage and use of the data in question.

In connection with a prior checking application, the Garante took the opportunity to clarify the data collection safeguards to be implemented by the companies offering interactive advertising services on digital terrestrial TV. The Garante ruled that collecting and using the data for such purposes was lawful on the condition that specific arrangements and measures were taken prior to offering the services in question. Reference was made, in particular, to the need for providing a detailed information notice via an ad-hoc screenshot prior to collecting the data, similar to both use of the data and the rights afforded to data subjects under the law. Where required, the consent must be free and specific – e.g. an ad-hoc key will have to be pressed. In no case may a company set up a centralised database; the data may be kept for a limited period (six months) and stringent security measures must be in place.

Media and respect for human dignity

In June 2006, the Garante took steps *ex officio* and issued a general provision setting out the requirements to be complied with following several instances in which newspapers had published transcripts of judicially authorised interceptions. The Garante stressed the need for reconciling a citizen's right to be informed and freedom of the press, on the one hand, with the respect for fundamental rights and freedoms of the individuals concerned on the other – particularly with their right to privacy. The wiretap records published in full actually contained passages concerning personal and/or family relationships, or victims of the relevant offences (third parties that were not the subject of the specific criminal investigations were involved in some cases). The Garante recalled the provisions in force and referred to the need for complying with the principle whereby only information that is material to the case must be published and no reference should be made to relatives or other individuals having no connections with the specific case; respect for human dignity should be paramount, and special safeguards are required in respect of the information concerning a person's sex life. The provision was addressed to all data controllers in the journalistic sector and published in the Official Journal. All media were called upon to perform a more careful, in-depth, autonomous, responsible analysis as to whether any details that are disclosed are actually material. In the Garante's view, the reduced privacy expectation of public figures and/or holders of public offices must be reconciled with the journalist's inescapable duty to protect human dignity and third parties' rights.

Latvia

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

Directive 95/46/EC

Amendments to the Personal Data Protection Law

To ensure the conformity of legal acts in Latvia to the requirements laid down in Directive 95/46/EC, the draft law 'Amendments to the Personal Data Protection Law' was elaborated in December 2005. The purpose of these amendments is to specify the personal data processing systems to be notified and the procedure of notification, creating the institution of data protection supervisors, to specify legal norms that have caused interpretation problems in the application of the law, and to specify the requirements of Directive 95/46/EC implemented in the Personal Data Protection Law. Thus it is foreseen that the Data State Inspectorate (DSI) would be able to pay more attention to control activities (including preventive control activities) rather than notification of systems. The draft law was accepted by the Government in August 2006.

Draft Law on Data State Inspectorate

In order to ensure full compliance to the provisions of the Directive 95/46/EC regarding the status of the personal data protection supervision institution in Latvia, discussions were organised within both the executive and academic sectors. An agreement was reached that there would not be a common 'umbrella' law adopted on all independent authorities in Latvia, but that an individual law should be adopted on every authority as it was justified that the authorities to be released from the subordination to the Cabinet are very different and, therefore, an individual and specific law in accordance with the actual circumstances is required.

Furthermore, regarding the determination of the status of independent institutions within the Constitution (Satversme), the Constitutional Court of Latvia by its decision on 16 October 2006 No. 2006-05-01 (the case of the National Radio and Television Board) has acknowledged that it is possible to have an institutional legal body that is not under the supervision of the Cabinet of Ministers. The Constitutional Court has provided the interpretation of Article 58 of the Constitution of the Republic of Latvia (Satversme along with other articles of the Constitution and has made a conclusion that strengthens the opinion that the Parliament has rights to adopt a law thus determining that an institution can legally be taken 'out' from the supervision of the Cabinet of Ministers. This decision is taken into account by elaborating the Draft Law on the Data State Inspectorate.

Considering all the above-mentioned, to ensure the conformity of legal acts in Latvia to the requirements laid down in Directive 95/46/EC, the Cabinet of Ministers approved the strategy of the Ministry of Justice for the time period of 2007-2009. One of the priorities within this strategy is to ensure that the Data State Inspectorate (which is currently under the supervision of the Ministry of Justice) would become a fully independent institution. Therefore the Data State Inspectorate of Latvia elaborated a draft 'Law on the Data State Inspectorate' which was submitted to the Ministry of Justice on 3 January 2007. It is foreseen that the forthcoming year (2007) will be very closely linked with the legislative

acts coming into force that will ensure the independence of the Data State Inspectorate of Latvia in compliance with Directive 95/46/EC.

Amendments to the Criminal Law
Latvia has been evaluating the liabilities with regard to the violations in the processing of personal data. The administrative liability is stipulated for violations in the processing of personal data – warnings, cash penalties, suspension of the personal data processing system and forfeit of the technical means used.

Furthermore it was decided to determine a criminal liability regarding the processing of personal data. The draft law, The Amendments to the Criminal Law, was approved by the Government on 29 January 2007. 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; if the aforesaid activities have been performed in order to take vengeance, blackmail or with other purpose, or if it is connected with violence, fraud or threats; and if the required technical and organisational means to protect personal data and prevent illegal processing has not been used and substantial damage has been incurred.

Currently the DSI evaluates the necessity to increase the level of administrative fines regarding the data protection misdemeanours in order to elaborate the amendment to the Administrative Penal Code.

Directive 2002/58/EC

Regarding the Directive 2002/58/EC, there have been amendments to the Administrative Penal Code adopted on 1 July 2006 that foresee the supervision regarding spam activities. This provision will come into force on 1 July 2007.

B. Major Case Law

Law on the Schengen Information System
The draft Law on the Schengen Information System was submitted to the government in September 2006. This draft law determines how the system will be used and the security measures regarding it, as well as the institutions that will ensure the functioning of the system and the supervision of personal data processing.

Law on the Processing of Biometric Data
The draft Law on the Processing of Biometric Data was elaborated in April 2006 and was approved by the Government on 2 January 2007. The purpose of this law is to ensure the establishment of a unified biometric data processing system.

C. Major Specific Issues

Schengen *acquis* implementation evaluation on data protection
The Schengen evaluation of the new Member States was conducted on 2006. Latvia had the Schengen experts' evaluation visit on 19-20 September 2006. During this visit experts proposed recommendations in order for Latvia to comply with the requirements of the Schengen *acquis*. This issue is one of the priorities for the Government of Latvia and the DSI in 2006 and 2007 (especially concerning the independent status of the DSI).

On 1 November 2006 there was a new division established within the DSI, the Data Protection Supervision Division of the Third Pillar, so as to

ensure the implementation of the Schengen *acquis* and supervision of data protection regarding law enforcement institutions.

General information

In 2006, one hundred thirty three complaints from natural and legal persons were submitted to the Data State Inspectorate. Ninety of these complaints were related to the presumable violations regarding personal data processing, mainly regarding data processing without a legal base, violation of the proportionality principle and violation of data subjects' rights.

With regard to the received complaints, control activities were carried out by the DSI. During 2006, it was concluded that from the 90 inspections carried out, 21 showed a violation of the Personal Data Protection Law.

The decisions made by the DSI can be appealed in Court (Article 31 of the Personal Data Protection Law). During the year 2006, two decisions were contravened and four decisions regarding administrative cases were appealed.

The DSI carried out several unexpected inspections, some of them based on the television news. For instance, there was a great debate in the country concerning the public holidays that take place during weekends. One television channel decided to launch a campaign – *Sign for the holiday* – where people had a chance to give their vote for this initiative by signing a list in one of the supermarket chain stores. The list was publicly available (just laid on the counters) and included personal data but no consent was given for the data subjects to agree to make their data public.

Other issues

- The Additional Protocol to Convention No. 108 regarding supervisory authorities and trans-border data flows in February 2007 was approved by the Government.

- Due to the amendments to the Personal Data Protection Law there will be changes regarding the notification on the data processing that will take place in 2007. However, the DSI has started the necessary assignments in 2006, in order to introduce the data supervisor alternative to the notification of data processing systems. This alternative will allow for an increase of administrative capacity in the DSI regarding the supervision activities, thus allowing it to become more pro-active than re-active, by putting a greater emphasis on preventive control activities.

Lithuania

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

1. The State Data Protection Inspectorate prepared the Rules of Prior Checking that were approved by order of Inspectorate Director No. 1T-6 of 2 February 2006. The rules specify the content of the notification, its submitting and the performance procedure for prior checking.

2. Following the Resolution of the Government of the Republic of Lithuania No. 1317 of 7 December 2005 on 'the Amendment of 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', the State Data Protection Inspectorate drafted a new recommendable form of notification on data processing.

3. On 25 May 2006 an amendment of the Law on the Population Register was adopted, establishing that facial images, fingerprints and personal signatures shall be stored in the Population Register. The data indicated may be disclosed only to law enforcement institutions and institutions issuing personal identity documents.

B. Major case law

Direct marketing

The State Data Protection Inspectorate is receiving increasingly more complaints related to the offering of goods and services by telephone, post or by other direct ways to people without their consent.

One applicant complained about the promotions carried out by the telecommunications company. Calls were being made to people, using randomly selected numbers, asking them to listen to information about various agencies' proposed services and, upon the person's consent, the latter was invited to subscribe to the telecommunications company. The described actions were being completed during a single telephone conversation. Paragraph 1 of Article 68 of the Law on Electronic Communications establishes that the use of electronic communications services, including electronic mail, for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. During the investigation it was determined that the telecommunications company had no prior consent. The State Data Protection Inspectorate drew up the protocol on administrative offences to the telecommunications company. The Court of Primary Jurisdiction, upon hearing the administrative case, concluded that the Law on Electronic Communications establishing the authorisation to use electronic communications services for the purposes of direct marketing (commercial purposes) with the prior consent of the subscriber, does not define the concept of the prior consent, the way of obtaining it, and the term which might imply that consent should be considered obtained in advance. Therefore the prior consent also applies in the case when calling to randomly selected telephone numbers and the subscriber's consent should be obtained at the start of the conversation before listening to information on proposed services. The Supreme Administrative Court of Lithuania, after hearing an appeal, decided that the subscriber's consent to use the electronic communications services for the purposes of direct marketing in terms of paragraph 1 of Article 68 of the Law on

Electronic Communications should be obtained (received) prior to the means deployed for the direct marketing but not at the (same) time.

Thirteen complaints were received concerning a book publisher, which sent out offers to people to enter a game without their consent. This company, on the terms of a subcontract, assigned a private enterprise to collect the personal data of potential clients, store them and administer the database. The latter bought personal data from other private companies, which had personal data collected from public resources. When performing the inspection on the lawfulness of personal data processing, the State Data Protection Inspectorate drew up a protocol on administrative offences committed by the head of the book publisher on the grounds that personal data were processed for the purposes of direct marketing without having the consent of the persons involved and that these persons were not informed about such processing. When hearing the administrative case, the question arose as to who was the data controller: was it the book publisher which was obligated by contract to the private enterprise to collect personal data, or was it the private company (enterprise) which was assigned to collect personal data? The court decided that the data controller was the book publisher, since the contract included the clearly defined purpose of data collecting and further processing (selling of goods for the purposes of direct marketing, the means of processing) and the creation of databases.

The principles of data processing

An increasing number of problems are arising concerning the administrative prosecution of people for infringement of general principles of data processing. Paragraph 1 subparagraph 4 of Article 3 of the Law on Legal Protection of Personal Data envisages that personal data shall be identical, adequate and not excessive in relation to the purposes for which they are collected and processed. The State Data Protection Inspectorate drew up a protocol on administrative offences for infringement of this principle of data processing because one private company collected an excessive personal data element – the personal identification number, which was not necessary for the data controller's purposes (accountancy). The Supreme Administrative Court of Lithuania stated that the interpretation of general principles, due exclusively to the nature of legal regulation, cannot be clearly defined, precise and uniform. In addition, the principles specified in the law, as well as the purposes, regulatory scope and other general introductory provisions of the law as a rule are explained and applied systematically together with other legal regulations. A direct application of regulations of a common declarative nature becomes especially questionable when defining actions entailing legal responsibility of a prosecutable aspect. Administrative responsibility may occur only for disregard of explicitly and unambiguously formulated prohibitions, but not for infringement of general principles. Therefore administrative prosecution for the infringement of general principles without alleging breaches of specific prohibitions is not possible.

C. Major specific issues

Tapping conversations in banks

The State Data Protection Inspectorate carried out inspections in banks in relation to the recording of clients' conversations. During the inspection it was determined that the majority of banks are making recordings of telephone conversations, both of bank workers calling

existing clients and of people (whether or not a client) calling the bank. Usually the outgoing telephone calls are recorded for the purpose of providing evidence of a commercial transaction or business communication. In most cases, bank clients have been informed about telephone recordings and have signed a contract with the bank to that effect. However, it was determined that there are some bank clients who have not signed a contract and who are not informed that their bank conversations are recorded or for what purpose. Several banks kepts records of incoming calls made either by bank clients or other persons to specially dedicated numbers accessible to the publicprovided for the purposes of obtaining information about bank services or making enquiries concerning existing contracts with the bank. Where these calls did not concern contracts, the identity of the caller was not revealed, however the number from which the call was made was recorded. During the inspection it was determined that the consent of the callers is not obtained and they are unaware of the conversations being recorded. These telephone calls are not related to the purpose of providing evidence of a commercial transaction or of any other business communication. Pursuant to paragraph 1 of Article 63 of Law on Electronic Communications, the bank may record a telephone conversation when the call is for obtaining information or consultation but only with the caller's consent. Since the inspections, the banks have improved the former situation, the bank clients are informed about the telephone conversations being recorded and the purpose of recording, and are giving the opportunity to discontinue the call if they so wish.

Inspections in consular authorities

The State Data Protection Inspectorate carried out inspections in the Lithuanian Consulate in Kaliningrad (Russian Federation) and the Lithuanian Embassy in Kiev (the Ukraine). They reviewed how the personal data of people applying for Lithuanian visas were processed, particularly concerning the issuance of simplified transit documents. During the inspection it was determined that the processing of personal data was not specified with regard to the preregistration system, the issuance system for simplified transit documents and the procedure of personal data destruction. Also the data storage duration was not established for the consular procedure management system, the preregistration system and the issuance system for simplified transit documents. It was also revealed that data subjects were not properly informed about their rights.

International data flow

The State Data Protection Inspectorate granted authorisation to the company conducting genealogical research to provide personal data to the United States of America. Personal data will be disclosed under the Personal Data Disclosure Contract between the company conducting genealogical research and the person involved, residing in the USA, who has ordered a genealogical research. The contract specifies adequate safeguards for the protection of an individual's right to privacy, as well as for protection and exercise of the other rights of the data subject, and organisational measures for the protection of personal data against any accidental or unlawful destruction, alteration, disclosure and any other unlawful processing.

Public awareness

At the end of September 2006 a press conference was held with the Committee on Legal Affairs of the Parliament (the Seimas) and the State Data Protection Inspectorate on 'The situation of data

protection in Lithuania'. At the conference the major trends of inspectorate activities and their results were presented, including a presentation of the survey of the inhabitants of Lithuania on data protection issues, an evaluation of Lithuania's preparedness to apply Schengen acquis in the field of data protection which was discussed, and a review of the inspections carried out by the inspectorate on the recording of telephone conversations in banks operating in Lithuania.

In November 2006 a conference entitled 'Legal regulation of personal data protection: problems and perspective' was organised by the Seimas Committee of the Development of Information Society. The guidelines of the draft law amending the Law on Legal Protection of Personal Data was presented, which had been drafted by the State Data Protection Inspectorate. The conference also covered personal data processing and protection issues in Lithuania.

Aiming to enhance public awareness and information to data controllers about data protection, the State Data Protection Inspectorate organised seminars on topical data protection issues to law enforcement institutions, educational, development and registry office institutions, and also institutions working with juvenile offenders. Round table discussions with diverse data controllers to facilitate the solution of problems in the area of data protection were also held.

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 (implementation of Directive 95/46/CE)

The bill relating to the modification of certain provisions of the framework data protection law, on which the Commission nationale pour la protection des données (CNPD) had advised the Government in 2005, has been filed with Parliament on 23 March 2006. Except for five opinions emitted by the relevant advisory bodies, no further developments have been made.

The future law will provide for more extensive exemptions for notification requirements and certain data processing will no more 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)

Minor changes to the provisions of the law of 30 May 2005 shall be implemented after adoption by Parliament of the aforementioned bill.

- Decrees and secondary legislation

No secondary legislation or decrees in respect of the above-mentioned laws have been taken during 2006.

- Other legislative developments

The law of 31 July 2006, implementing a unified Code on Labour Law, abrogated certain provisions related to the surveillance at the workplace from the law of 2 August 2002 on data protection, in order to implement them into the Labour Law Code for the sake of unification and codification.

The bill regarding the use of genetic data for the identification of persons in the domains of law enforcement and criminal law, on which the CNPD had advised the Government in 2004, came into effect by a law dated 25 August 2006.

B. Major case law

- Civil and criminal case law

Court of Appeal of Luxembourg, 8th labour chamber on the validity of proofs (access control system) collected in violation of the law of 2002 on data protection

The Court of Appeal of Luxembourg in labour matters ruled on 26 January 2006 that a dismissal on the grounds of non-respect of the working hours was justified, although no prior authorisation from the CNPD had been granted for the access control system. The appellant argued, among others, that the employer misused such a system, as no prior authorisation had been granted by the CNPD and that the proof provided by the employer had therefore to be discarded from the court hearings. The Court of Appeal rejected this argument, by stating that even if the employer had violated the provisions of the law on data protection; such violation neither jeopardized his right to an equitable trial, nor interfered on the reliability of the proof, which had been debated among the parties.

It should be noted that the solution adopted by the Court of Appeal did not meet the acceptance of the Luxembourg doctrine. Reference must also be made to the judgment of the District Court of Luxembourg, 9th correctional chamber dated 13 July 2006, which adopted the exact opposite view.

District Court of Luxembourg, 9th correctional chamber on the validity of proofs (video-surveillance images) collected in violation of the law of 2002 on data protection

On 13 July 2006, the 9th correctional chamber of the District Court of Luxembourg ruled that, in a penal matter, proof obtained or collected in violation of the law of 2002 on data protection, is inadmissible and must be discarded from the proceedings. The case related to a public video-surveillance which was executed by a company without having received prior authorisation from the CNPD. The judges ruled that, without such prior authorisation, the proof obtained had to be declared illegal. As the proof was discarded, the whole prosecution was void, as it was entirely based on these video-surveillance images. The case is currently pending at the Court of Appeal.

It should also be noted that, in a decision dated 11 October 2005, the Court of Appeal, 5th correctional chamber, in a very similar matter (video-surveillance at the workplace without having received prior authorisation from the CNPD), had adopted the exact opposite position of the above ruling - the use of the proof obtained irregularly and in contempt of the provisions of the law of 2002 on data protection was admitted by the judges during the proceedings.

- Administrative case law

For the year 2006, there are no Court decisions to report regarding the application of the Data Protection Law in respect of administrative law matters.

C. Major specific issues

The CNPD granted its first authorisation for the installation of a biometric system used for the purpose of access control in an important wellness and fitness centre. Such a system had been refused in 2005 as the storage of biometric data in a central database was excessive in relation to the purpose of access control. The applicant aligned his system to the requirements imposed by the CNPD. The central database has been replaced by a system storing the biometric data exclusively on a secured badge which remains under the control of the data subject.

During 2006, the CNPD carried out an exhaustive audit concerning security measures taken by the main public healthcare and pension insurance bodies. The aim pursued by the CNPD was to obtain an overview of how health-related data are processed and if the rights of the data subjects are respected by the data controller and its processor. The CNPD made comprehensive recommendations and guidelines and granted the necessary authorisations to the audited bodies.

The Grand-Ducal decree on biometrical passports came into force on 31 July 2006. The CNPD provided extensive guidance to the relevant authorities and public entities on technical as well as practical aspects of biometrical documents.

The CNPD pursued its information and awareness raising campaign by publishing in early January 2006 a calendar on data protection, in collaboration with the Luxembourg consumer association.

Malta

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

Directive 95/46/EC was transposed in Maltese legislation under the Data Protection Act; Chapter 440 of the Laws of Malta. The Act was completely brought into effect in July 2003, establishing a transitional period for notification of automated processing operations by July 2004. Certain provisions in relation to manual filing systems will be effective by October 2007.

Directive 2002/58/EC was transposed partly under the Data Protection Act, by virtue of Legal Notice 16 of 2003, and also under the Electronic Communications Act by virtue of LN 19 of 2003; both subsidiary legislation were brought into force in July 2003.

Other legislative developments

None to report.

B. Major case law

A junior Minister filed a complaint with the Office in relation to a case where a journalist, who identified herself as a normal citizen, called the Minister at his private office and requested an appointment for consultancy services. The investigation being carried out by the journalist was to entrap the Minister in an alleged case of the carrying out of private work against remuneration; this in contravention to the code of ethics for Ministers and Parliamentary Secretaries. The telephone call was transmitted on the opposition's party television station. The Commissioner put in the balance the right to privacy of the Minister against the freedom of expression exercisable by the journalist. Specific considerations were also made to the fact that the Minister is a public figure performing public duties and also to right of the public to be informed of such cases. Similar judgements delivered by the European Court for Human Rights were also factored in the examination of the case. The Commissioner concluded that freedom of expression exercised by the journalist to inform the general public prevailed over the right to privacy of the Minister. The decision was not appealed.

The office also received a request for prior checking by the mobile phone providers requesting guidance from the Commissioner in relation to a request for disclosure of subscribers' traffic and location data by the Police in the course of an investigation. This, subsequent to a spate of arson attacks carried out on members of the media namely a journalist and a columnist in a leading paper. In his decision, the Commissioner considered that such attacks constituted a threat to public security and therefore authorised the service providers to provide, under specific conditions, the Police with the requested data. This decision was appealed by the service providers before the Data Protection Appeals Tribunal. The Tribunal decided in favour of the Commissioner. The parties felt aggrieved by such a decision and according to the provisions of the Data Protection Act appealed, on a point of law, before the Court of Appeal. The case is still for hearing before the Court.

C. Major specific issues

During 2006, the Commissioner held regular meetings with representatives from the various sectors to discuss data protection issues and develop guidelines regulating the processing of data in the relative various

sectors. These included financial institutions, journalism, insurance, social welfare, education and Police. Discussions were also initiated with representatives from two other sectors, the photographers and security service sectors, where specific matters required the intervention of the Commissioner to ascertain that privacy rights were being safeguarded. It is envisaged that guidelines in these sectors will be developed by the end of next year. In February the guidelines for the promotion of good practice in the insurance business sector, developed in conjunction with the Malta Insurance Association, the Association of Insurance Brokers and MFSA, were launched during an information session. These guidelines refer to the processing operations in the insurance business relating to the preparation and issue of insurance policies, premiums, settling of claims and reinsurance. The Office maintained close co-operation with other regulatory authorities, associations and federations.

On 25 January the Office's new portal was officially launched by the Minister for Investment, Industry and Information Technology during a press conference held at the Office. The new system was developed as part of the e-Government programme. This system provides the general public with online services and caters for back-office facilities to ease the administrative workload so that human resources could be better utilised on core technical data protection matters.

During this year, the Office continued with the implementation of the twinning light project which commenced in October 2005 with the German Federal Commissioner for Data Protection. The global objectives were to assist the Commissioner to strengthen the expertise to fulfil his duties and obligations in the administration of the Data Protection Act and also assist the Data Protection Unit within the Office of the Prime Minister to enhance data protection skills in the Public Service. The twinning agreement was concluded on 3 June. The programme rendered significant positive results both in terms of knowledge transfer and in the adoption of concrete recommendations delivered by the various experts in the areas of competence. During the period, experts were attached to the Office as part of the team; in that, they participated in meetings, advised the Commissioner on resolution of complaints and were also involved during inspection visits. Further to the twinning project, this Office has further strengthened the relationship with the German counterparts.

As part of Malta's preparations for accession to Schengen, the Office was subject to a peer review carried out by the Schengen Evaluation Data Protection Committee composed of 12 European evaluators. Experts called at the Office to evaluate the internal operations and procedures, in particular the exercise of the Commissioner's supervisory role. Presentations by the Commissioner, technical staff and the data protection officer within the Ministry of Foreign Affairs were made. The outcome of the evaluation was presented to the Schengen Working Party during the Council meeting where the Data Protection Authority was given high marks for being adequately geared to exercise the role of data protection regulator on all data controllers including the Police. The Office commenced the regular inspections of Police systems, where the first in a series were carried out with the assistance of German IT experts. Such systems are inspected to ensure

that the maximum level of security is in place to safeguard personal data against unauthorised access and to ascertain that these are complaint with other European obligations; in certain cases recommendations were made. As part of the regulatory functions, the Commissioner is also expected to carry out inspections on data controllers. 14 inspections were carried out and these included the Maltese Embassies and Consular Offices in Tunis and Moscow.

The Netherlands

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

Directive 95/46/EC was transposed into national law by an act of 6 July 2000[1] 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 transposed into Dutch law mainly by the changed *Telecommunicatiewet* (Telecommunications Act) that entered into force on 19 May 2004[2]. Other legislation transposing parts of this directive are amongst others in the *Wet op de Economische Delicten* (Act on Economic Offences), that implements article 13(4) of Directive 2002/58/EC.

B. Major case law and major issues

The work of the Dutch Data Protection Authority, College Bescherming Persoonsgegevens (CBP), has covered many different areas and topics during 2006. In this report, four of these areas, considered crucial, are highlighted: the area of justice, security and control, large-scale processing of personal data, the prevention and detection of fraud, and the Internet. From each of these areas, one or more developments will be elaborated.

1. Justice, security and control

Investigation of terrorism

Police and justice authorities have been given increased powers in recent years, with the aim of fighting terrorism. The Dutch Data Protection Authority (DPA) has advised the Minister of Justice and Parliament on the proposal for an act that would enlarge the possibilities for the investigation and prosecution of terrorist crimes. The DPA criticised in particular the lack of sound argumentation for the necessity of the proposed measures. One of the measures proposed is the possibility of larger exploratory investigations of certain groups in society. Because the criticism of the DPA was put aside, upon request of the President of the Senate, the DPA has given further advice to the Justice Commission of the Senate about the measures that would be necessary to reach a better balance between supervision on the processing of personal data and the increasing powers of the police and justice authorities.

Theme processing

The new act on the processing of police records, entailing a radical review of the Police Files Act *(Wet politieregisters)*, will undoubtedly have consequences for data protection. One of the major changes is the introduction of the so-called 'theme processing'. In a theme processing, the personal data of unsuspected people, against whom there is no reasonable suspicion of guilt (based on facts and circumstances), can be systematically and pro-actively processed. The DPA has warned that without extra data protection measures, such as coding, there is an unacceptably large danger that civilians will become the object of unjustified police action. The DPA has also highlighted the necessity of permanent control of the correctness and quality of police data.

[1] 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

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

2. Large-scale data processing

Because of the advancing technological developments, it becomes increasingly easy for organisations in both the public and private sectors to process personal data on a very large scale. This can be convenient and lucrative; however it can also be very damaging for individuals, particularly when mistakes are made. The crucial matter is to ensure a good design of new processing systems from the outset, from both a technical and a legal point of view.

The Citizens' Service Number and the Electronic Health File

The introduction of the Citizens' Service Number *(Burger Service Nummer, BSN)* has been a recurrent theme over the last couple of years. The introduction was planned for 2006, but has been postponed until 2008 when it will be introduced gradually, by replacing firstly the current social-fiscal number in the health sector. Since its first advice on the proposal in 2004, the DPA is still discussing with the Minister and Parliament the necessity to build safeguards into essential parts of the legislation to ensure fair and lawful processing of personal data. When a mistake is made in one of the back offices with regard to the BSN, the consequences for the individual can be tremendous, due to the linking of many administrative systems. The act does not provide for sufficient measures for reparation in case of mistakes. This is damaging for the trust that a citizen should be able to have in the processing of his personal data by the Government.

In the health sector, the BSN will be used to enable the Electronic Health File. The DPA is actively involved in the development of this file. The main issues are ensuring a good division of responsibilities, access, security and supervision.

The travel card

The Government intends to introduce one travel card for all public transport in the Netherlands. In 2006, the Dutch DPA voiced substantial criticism against the use that transport companies intend to make of personal travel data for the purposes of service provision and direct marketing. This has led the Parliament to insist that the Minister solves the privacy issues at stake. Responding to Parliament's demands, the Minister has tried to identify and solve several privacy bottlenecks in consultation with the transport companies and the Dutch DPA. In 2007, the Dutch DPA will investigate a transport company that has partly introduced the travel card to identify if and how measures to protect personal data have been taken.

3. Fraud prevention

Prevention of fraud in social welfare

To avoid abuse of public funds, more and more municipalities want to verify with other organisations the information provided by clients when requesting social welfare. In addition to that, linking data with other databases is also increasingly used as a means to fight fraud. In reaction to this development, the DPA produced a vision report in 2006 on fraud prevention through the linking of databases, which provides guidance for finding the right balance between fraud prevention and respect of privacy.

Fraud in housing

In the fight against fraud in housing by people on social welfare, municipalities can demand information on gas, water and electricity use from the relevant companies. In addition to that, one local authority had planned to link the garbage administration to the administration

of the social welfare service, in order to get an indication of the occupation of a house. The DPA has judged that this practice is not allowed; the municipality has not been able to prove that these measures, in addition to already existing measures which include personal visits, are necessary. Furthermore, the garbage administration is used for billing purposes; further use for fraud prevention is incompatible.

Intervention teams

In order to fight fraud in social welfare, several public authorities co-operate in so-called 'intervention teams'. In certain cases these teams also collect the personal data of citizens through observation, without the citizens being informed of this. However, the Data Protection Act obliges the organisations to inform citizens of this practice, and also if no incriminating data have been found. A renewed protocol for this practice has been approved by the DPA in 2006. The DPA also prepared an investigation to be undertaken by several intervention teams in 2007.

4. Internet

Publications on the Internet

The DPA has taken stock of the daily problems some people face resulting from publications about them on the Internet. A definite legal analysis of what is and what is not allowed with regard to Internet publication has proven difficult to make, due to the complexity of the matter. In 2006, the DPA has developed a provisional policy, which is also aimed at stimulating the debate about this topic with a wider audience. This policy has been published in a report that was presented at the farewell conference of the DPA's commissioner, Jan Willem Broekema. Based on discussions about and experiences with the provisional policy in 2006, the DPA will publish guidelines early in 2007 on the processing of personal data in publications on the Internet.

Personalised Internet services

The use of personalised services on the Internet, such as Gmail, provides the service providers with ever larger personal 'data warehouses', including information on Internet searches, e-mail content or even the content of computer hard disks. The provision of these data to third parties, including those based on government demands, could have enormous consequences for individuals.

In a public debate organised by the DPA and the consumer organisation, Google Europe acknowledged that IP addresses are indeed, in many instances, personal data, which implies that the data protection law fully applies to them. The DPA emphasised that the use of these data for other purposes is allowed only in certain cases, that individuals should be duly informed of the use made of their data, and that users have a right to access their data and correct them. Finally, a maximum storage limit must be maintained.

Poland

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

The amendment to the Act on Telecommunications Law (Journal of Laws No. 171, item 1800) entered into force in February 2006. It related among others to the contents of Article 165 paragraph 1 of the Telecommunications Law, in which the storage period of traffic data was extended from one to two years. In the discussion period other proposals for further extension of the traffic data storage period were presented but they were not accepted.

In 2006, work on the amendments to the Telecommunications Law began, which would ensure full transposition into Polish legal order *inter alia* of the provisions of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as well as Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC. The works on the planned changes of the provisions are continuing. The amendments will probably be approved in 2007.

B. Major case law

Public figures' privacy

On 20 March 2006 the Constitutional Tribunal at the request of the President of the Supreme Administrative Court concerning limitation of the protection of the right to privacy of a public figure fulfilling public functions stated that Article 5 paragraph 2 sentence 2 of the Act of 6 September 2001 on access to public information is compliant with the Constitution. Pursuant to Article 5 paragraph 2, 'The right to public information is limited in order to protect the privacy of a natural person or entrepreneur's secrecy' – and the challenged sentence states that 'The limitation shall not concern information on persons fulfilling public functions in regard that the information is connected with fulfilling the function including the information on conditions of entrusting and performing the function, and in the case where a natural person or entrepreneur gives up the right.'

In the tribunal's view, privacy can in specific circumstances be subjected to interference carried out for public interest. However, such interference shall be carried out in a careful and balanced way with due evaluation of the arguments supporting it. One needs to remember that these interests are equiponderant.

The Constitutional Tribunal stated that the challenged provision of the act on access to public information would be inconsistent with the Constitution only if its application violated the above-mentioned principles. This means that the information disclosed by means of access to public information cannot go beyond what is necessary for transparency of public life in accordance with the standards adopted in a democratic state of law. Disclosed information shall not violate the essence of the protection of the right to private life. Thus it always has to be of importance for the evaluation of the institution's functioning and the people fulfilling public functions.

Limiting the freedom of speech

On 19 October 2006, the Constitutional Tribunal decided that Article 212 § 1 and 2 of the Act of 6 June 1997, the Penal Code, is compliant with the Constitution. Pursuant to this Article: 'Anyone who defames another person, a group of people, an institution, a legal entity or organisational unit without legal personality by attributing them an act or a characteristic which may abase them in the eyes of public opinion or jeopardise the loss of confidence necessary to carry out a certain post, profession or kind of activity is liable to a fine, restriction of personal liberty or up to one year's imprisonment.'

In the reasons for the judgment the Constitutional Tribunal stressed that citizens' rights and freedoms such as dignity, good reputation and privacy can in specific circumstances deserve taking precedence over freedom of speech and freedom of press, and in consequence led to their limitation.

The very fact of the legislator recognising it as an offence of a deed constituting a manifestation of enjoying the freedom of speech and at the same time violating the good reputation of a third party does not infringe the Constitution.

On 2 October 2006, the Supreme Court's Criminal Law Division rendered a judgment in which it expressly stated that criminal liability pursuant to Article 51 of the Act on Personal Data Protection (disclosure of personal data to unauthorised persons) for publishing personal data (e.g. address) in the press against the ban specified in Article 14 of the Act on Press Law shall be born by the editor-in-chief as the person who is obliged to protect these data by the act.

While analysing the relations between the Act on Personal Data Protection and the Press Law, whose Article 4 paragraph 6 provides that it is forbidden to publish the information and data regarding private life without the interested person's consent, unless it is directly related to the public activity of a specific person, the Supreme Court focused on the interpretation of the press clause included in Article 3a paragraph 2 of the Act on Personal Data Protection. Under this provision, except for the provisions of Article 14-19 of the Act on Personal Data Protection, it shall not apply to press journalistic activity within the meaning of the Act on Press Law and to literary or artistic activity, unless the freedom of expression and of distribution of information fundamentally violates the data subject's rights and freedoms.

The Supreme Court emphasised that the quoted Article 3a paragraph 2 does not mention Article 51 as the one to be applied to journalistic activity in the press, but it stipulates that the provisions of the act shall be applied if the freedom of distribution of information fundamentally violates the data subject's rights and freedoms. Whereas in the Court's view it is obvious that violation of the data protection rules by disclosure of data to unauthorised persons, as being subject to penalties, constitutes a fundamental breach of the right to privacy and with regard to such behaviour, the provision of Article 51 paragraph 1 shall also be applied to journalistic activity in the press. The Supreme Court noted that under Article 36 paragraph 1 of the Act on Personal Data Protection the editor-in-chief shall be obliged to protect personal data against disclosure to unauthorised persons. Thus he is the person obliged to the protection of personal data of everyone to

whom journalistic material published by his editorial team relates. The violation of this obligation bears the attributes of an offence within the meaning of Article 51 paragraph 1 of the Act on Personal Data Protection providing for punishment for disclosure of personal data to unauthorised persons by the person obliged to their protection.

Health data

On 5 August 2006, the Voivodeship Administrative Court in Warsaw dismissed a complaint against the decision of the Inspector General for Personal Data Protection, sharing the Inspector General's view that disclosure of the complainant's health data to a person carrying out a physician's profession and to a medical university for the purpose of drawing up an extrajudicial medical opinion concerning the complainant's state of health and processing this data while preparing this opinion, was necessary to assert the complainant's right to protection before court and found its legal basis in Article 27 paragraph 2 point 5 of the act. The Court recognised also the Inspector General's statement that the Data Protection Authority (DPA) is not competent to evaluate whether the physician preparing the opinion on the state of health violated the separate provisions providing that the physician can issue an opinion on the state of health after having personally examined a person as well grounded.

Associations

On 6 July 2006, the Voivodeship Administrative Court in Warsaw dismissed a complaint against the decision of the Inspector General for Personal Data Protection concerning the legality of processing the personal data of the complainant's daughter and the information on his family situation by the association.

The Court shared the Inspector General's view that the complainant upon concluding with the association, regarding a contract for gathering funds destined for helping his ill daughter, at the same time authorised the association to process her data on the website and in other informational and promotional materials of the association. Thus the association was entitled to process both any information on the daughter disclosed to it and information on the complainant's family situation for the purpose of obtaining funds for help related to rehabilitation, treatment, purchase of drugs, equipment, etc. It was obvious to the Court that in order to confirm the situation of a person awaiting help from the association, which in fact only acts as an intermediary in providing this help, it was necessary to prove that the beneficiary really needed this help. The credibility of the beneficiary's needs undoubtedly had to be evaluated with regard to her health, family and financial situation. At the same time, the Court agreed with the Inspector General that the challenged reliability of execution of the contract by the association cannot be subject to evaluation by an administrative body, because these are civil law issues.

C. Major specific issues

On 30 and 31 January 2006, a group of EU experts, according to the mandate given by the decision of the Standing Committee on the evaluation and implementation of the Schengen *acquis* of the Schengen Evaluation Working Group, visited Poland in order to conduct a periodical evaluation of the implementation of the Schengen acquis in Poland.

This mission was of special importance because a favourable evaluation is necessary in order

for Poland to join the Schengen Information System. During their stay in Poland the experts examined legal and factual preparations of the Polish DPA with regard to fulfilling the functions of a supervisory authority, referred to in Art. 114 paragraph 1 of the Convention implementing the Schengen Agreement.

The presented report shows that Poland is well prepared for accession to the Schengen Agreement in terms of issues regarding personal data protection. In particular it was stated that the legal position and the functioning of the Inspector General for Personal Data Protection ensure proper fulfilment of its supervisory authority's function.

It needs to be emphasised that the Inspector General actively participates in further preparations for Poland's accession to the Schengen Agreement.

As part of further activities the Inspector General performed inspections in selected consulates and drew attention to the authorities, which will have access to SIS in the future, to the need for proper fulfilment of the information obligation towards data subjects.

In 2006 the main problem featuring in complaints related to the banking sector was, as in previous years, the transfer by banks of data files kept by the Credit Bank Agency (BIK S.A.) and the Polish Banks Association, which is a bank obligation referred to in the provisions of the Banking Law. In most cases the complainants requested that the transfer be recognised as illegal and their data be erased from these files. In a few cases, the ungrounded processing of complainants' data in the file kept by BIK S.A. after the completion of an obligation linking the complainant with the bank was was found to have been unwarranted and the erasure of this data was ordered. However, in the majority of cases of this kind, the request to recognise the transfer of data as illegal was refused, as the complainant's obligation towards the bank existed at the time of deciding the case.

Among the cases concerning telecommunications, the Inspector General for Personal Data Protection has been dealing with such problems as the processing of traffic data. The Inspector General conducted administrative proceedings and ordered one mobile telephone provider to:

1) fulfil the obligation to inform subscribers with whom it concludes the contracts for providing telecommunications services as provided in the Telecommunications Law about: a) the scope of processing traffic data, and the possibilities of influencing the scope of such processing, b) the categories of traffic data processed for the purpose of calculating costs and payments and the time for which the data can be processed, c) the type of traffic data which will be processed for the purposes of telecommunication services marketing, the provision of value added services and the period of processing;
2) place a separate clause in the contract about the consent of a subscriber to the processing of his/her traffic data for the telecommunication services marketing purposes and to the processing of such data for the purpose of providing value added services, and provide the subscriber with the possibility to refuse to give consent to any of the above mentioned purposes.

One of the widely commented cases in 2006 concerned the actions of an entity which

sent invoices to the clients of a known telecommunications provider seemingly from that provider. At the same time this entity sent contracts based on which personal data were expected to be placed in the Internet phonebook. The Inspector General informed the prosecution bodies about the possible crime being committed due to the processing of personal data without legal grounds, failure to register the data filing system and failure to fulfil the information obligation.

One of the problems concerning operations on the Internet was the collection of more personal data than was required. This problem occurred, for example, in companies offering registration of Internet domains, which collected clients' personal data by copying their identification documents. Such documents include information such as appearance, family name, parents' names and, in the old versions, marital status. It needs to be emphasised that there were no prerequisites justifying the processing of the additional data included in the identification documents and the balance between the rights of the data subject to control his/her data and the interests of the controller in such cases was a concern.

Portugal

A) Implementation of Directives 95/46/EC and 2002/58/EC

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

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

During 2006, some legislation including data protection issues entered into force, in particular Law 51/2006 on the use of video surveillance and other electronic systems to monitor traffic, incidents and infringements on the highways. This law provides the possibility for highway companies to install these systems, as well as giving access to law enforcement authorities to process the data.

The new passport model was also approved, which includes biometric data. Both acts received the prior opinion of the Data Protection Authority (DPA).

The Portuguese DPA has been included, by legal disposition, as one of the competent authorities within the application of Article 4 of Regulation (EC) 2006/2004 of 27 October, to integrate the Consumer Protection Co-operation System (CPCS) where spam is concerned.

B) Major case law

We would like to highlight a decision, of February 2006, from the Supreme Court concerning the use of video surveillance in the workplace. Following the appeal of a trade union, the Portuguese Supreme Court decided to remove almost all video cameras as there was a disproportionate violation of workers' privacy at the workplace. Video surveillance at the workplace is admissible under the Labour Code for security reasons, and cannot be used to monitor the workers' performance. In this case, the company produces medicines and there was evidence of substances being stolen which may endanger public health. The Court considered that the workers could not be subject to a permanent 'police measure'. This Supreme Court decision was very important because, in a limited situation, it pended in favour of privacy. Likewise it guides the DPA intervention when assessing the proportionality of data processing by video surveillance.

Another key decision of 2006 was from the Administrative Supreme Court, following an appeal of the National Association of Pharmacies ("ASSOCIAÇÃO NACIONAL DE FARMÁCIAS") against a decision of the DPA, upon which the Central Administrative Court had already decided favourably.

The situation goes back to 1999, when the DPA did not grant authorisation for the National Association of Pharmacies to process, at national level, a huge amount of personal data, including all the medicines bought by every single person, a list of all physicians and their prescriptions and other information concerning the health system. The DPA considered then that there was no legal ground under the Portuguese Data Protection Act and it was clearly disproportionate for the Association to process this sensitive data.

The Administrative Supreme Court decided in favour of the DPA decision.

There were other smaller cases concerning appeals against the DPA's sanction decisions, in particular the application of pecuniary sanctions

for the lack of notification and the lack of the right to information from video surveillance systems. In 2006, the trend of a clear majority of court decisions in favour of the DPA was kept.

C) Major specific issues

1. Opinions to draft laws

Under the Data Protection Act, draft legislation, either at national or international level, which contains data protection matters, has to be submitted to the DPA for an opinion.

In 2006, the DPA provided 46 opinions, some of them related to legislation in preparation within EU bodies, such as the Framework Decision concerning the interchange of information contained in criminal records; the principle of availability; or the EU/USA agreement on passenger name record data. The DPA also gave opinions on the transposition of Directive 2004/52/EC about electronic tolls and Directive 2005/28/EC regarding experimental medicines for human use. In relation to other national legislation, the DPA issued opinions on several important matters closely related to data protection, such as video surveillance in taxis; disclosure of a tax debtors list; e-passport; control of driving under the influence of alcohol and psychoactive drugs; civil identification card (citizen card); criminal identification database; nationality ruling; entry, residence and exit of foreigners in national territory; public service of electronic mailboxes; healthcare network.

2. Front office

In 2006, the Portuguese DPA opened a front office, exclusively dedicated to assist data subjects and data controllers, either personally or in writing, by dealing with information requests, and by receiving notifications and other documentation. At the same time, the DPA launched a dedicated phone line, called the 'privacy line' (+351 (0)21 393 00 39) to provide assistance to the public in general. Information requests may be submitted by telephone, e-mail, fax, in writing or on the website.

The opening of a front office enabled a better rationalisation of the work and an improvement in the assistance provided and time of response.

3. Access by insurance companies to health data of the deceased

The Portuguese DPA receives many access requests to health records of deceased people within the framework of life insurance contracts. Insurance companies want access to this health data in order to pay the insurance beneficiaries of the deceased

The DPA issued guidelines in 2001 about access to health data from third parties, allowing only insurance companies to get information on the cause of death and nothing else, if there was no consent from the data subject. Other requests have been received for access to health records from insurance companies, based on contractual clauses signed by the deceased. The DPA evaluated the situation and concluded those contractual clauses do not substantiate a specific and informed consent from the data subject. Following this assessment, the DPA recommended that insurance companies get an autonomous contractual clause, requiring a separate signature, specifically informing the data subject/insurance applicant of the purpose of the access and collecting his/her consent. However, the DPA considers that insurance companies should only have access to the cause and evolution of the disease that caused the

death and not the entire health record, which could enable insurance companies to verify if there was contractual bad faith, and therefore refuse to pay the due compensation. The deliberation is available at **www.cnpd.pt**

4. Medicine at the workplace

In 2006, the Portuguese DPA approved a standard authorisation on workers' health data processing for the purpose of security and medicine at the workplace. The employer does not have any access to workers' health data, only the information provided by the workplace doctor, such as 'fit' or 'unfit' to work. The DPA also appreciated the data related to alcohol and drug tests, which are only admissible on a regular basis in some particular professions if there is risk for human life.

Security measures and data storage periods were also dealt with, as well as the data processed by outsourcers. This standard authorisation intends to provide guidance to data controllers in this area and to raise awareness among employees about their rights. It is available on our website at **www.cnpd.pt**

Slovakia

A. Implementation of Directive 95/46/EC and other legislative developments

Implementation of Directive 95/46/EC

In February 2006, a two-day negotiation was held between the deputy of the European Commission and the representatives of the Office for Personal Data Protection in Slovakia (hereinafter the 'Office') when the harmonisation of the amended Slovak Act on the protection of personal data with Directive 95/46/EC was evaluated. This was the first bilateral meeting held after joining the European Union and was aimed at fully harmonising the national legislation with the requirements of the directive.

In January 2007, the Slovak Data Protection Authority (DPA) received a report from the Directorate-General for Justice, Freedom and Security of the European Commission in which it expressed that the situation in Slovakia regarding data protection is satisfactory. Act No. 428/2002 Coll. on the protection of personal data was amended by the Act No. 90/2005 Coll. (hereinafter the 'Act on Personal Data Protection') and the Slovak DPA will execute its function in spite of limited financial as well as human resources.

A positive development in the data protection field has been recorded in Slovakia. Even though it is necessary to improve the independence of the DPA, the issues of the office's finances, competences and its constitutional incorporation would be answered and several amendments of the act would be executed in order to achieve full harmonisation with the data protection directive. The Act on Personal Data Protection should be amended in such a way that the Slovak DPA gets more investigative powers. The recommendations of the Commission will be a subject of a restatement of the act which is intended to be realised during 2007.

Other legislative developments

The office within the 'legislative proceedings on draft acts' commented on 156 drafts, acts, regulations and ordinances of the Government of Slovakia. The most frequent drafts were proposals from the Ministry of Interior, the Ministry of Health and the Ministry of Finance.

Generally the comments of the office were accepted except for the case where there was conflict on the wording in the Act on Banks on the data retention period; the Parliament decided in favour of the Ministry of Finance. According to the new wording, the records from monitoring bank premises shall be destroyed after 12 months.

Following a proposal from the DPA, an important amendment to the Act on Public Health was executed. The DPA enforced that the personal data included on medical reports are enumerated by the above-mentioned act.

B. Major case law

In 2006, three cases were put before the court: two of them were against an order issued by the Office because of violation of the Data Protection Act and one of them was initiated by a Swiss citizen who sued the Office allegedly for its inaction because his personal data were disclosed on the web page of certain journal.

In the first case, a banking institution had adopted measures against clients before there was any legal base in place for such conduct and the act in question became effective later on. The regional court has further issued a verdict wherein the case would be put in cessation. Eventually a consent decree between the Office and the respective banking institution was approved.

In the second case the Office issued an order against the unauthorised transfer of personal data from a privatised institution to newly formed one as there was no contractual base for the transfer of personal data. The subject matter was resolved by a verdict of the Court that the request contained in the order of the Office was not justified.

Regarding the third case, legal proceedings are not closed at the time of writing. The decision of the Slovak Supreme Court on the question as to whether the Office as defendant should have had legitimacy to take actions against the public disclosure of already-published personal data of a petitioner on the website of a Slovak journal is to be expected soon.

C. Major specific issues

In the year 2006, there were 102 notifications to the Office from filed data subjects and other natural persons who alleged that their rights stipulated by the Data Protection Act had been directly infringed. Twelve notifications were filed by other subjects who announced suspicion of a violation of the Data Protection Act. Eighty-two proceedings were conducted *ex officio*. These 196 notifications amounted to an increase of 55% on 2005.

In 2006, the inspection department carried out 96 inspections and 'requests to explanation' and 70 binding orders were issued.

Observing Government Resolution No. 558/2006 on the preliminary opinion of Slovakia towards the evaluation report about the compliance of the personal data protection provisions with the provisions of the Schengen *acquis*, the Office conducted inspections in the consular departments of the diplomatic representational bodies of Slovakia in Ukraine, Belarus and the Russian Federation as well as in the Ministry of Foreign Affairs in Slovakia.

Processing of personal data of a commercial insurance company's clients

The Office dealt with a case related to the violation of rights of a commercial insurance company's clients. The investigation of the case was prompted by an article published in a national journal. This journal was addressed by a reader who had received a database by e-mail containing the personal data of about 20 000 clients including their details as car owners: their personal identification number, automobile type and mark and also the price that these owners had paid for mandatory contractual insurance in 2005. The receiver of this huge database was not the person with authorised access and the data had been sent to him in error by a responsible person at the insurance company. Fortunately the person who informed the journal provided for the security of the received personal data. As the Office found there had been no misuse of the data no fine was imposed.

Processing of personal data while providing accommodation to foreigners

The Office dealt with several cases of suspected illegitimate processing of visiting foreigners' personal data. A number of controllers obtained the personal data of foreigners illegitimately

by photocopying their personal documents without their consent and some did not ensure that the hotel booking information only contained the personal data necessary for that process. The excessive personal data processed for the purposes of accommodation were, for example, their occupation, their employer's details, personal identification number and place of birth. The Office issued an order so as to eliminate this happening again.

Processing of a patient's medical documentation during transportation

The Office dealt with a case of insufficient protection of personal data during the transportation of a patient from one hospital to another. The medical documentation of a patient was given into the custody of an ambulance driver who put it on the vehicle roof and forgot to remove it before driving away. According to the act on healthcare and healthcare-related services, a healthcare services provider as the controller of an information system is fully responsible for medical documentation. It was found that a contract on processing the personal data by a processor (which in this particular case was the Transportation Healthcare Service) was not in place. The Office defined the provider of the healthcare as the controller of the information system fully accountable for the lost documentation. The Office has informed the Ministry of Health of the case and asked for issuance of a uniform regulation for all medical institutions which should contain guidelines on how to handle medical documentation in such situations.

Income (Pension) administration funds

The Office initiated a proceeding on the merit of an illegitimate provision of personal data by the controller of a pension administration fund. According to the Act on old-age pension savings, the pension administration fund is now obliged to inform savers about the state of their pension savings account. However, pension administration funds used to send extracts of the accounts by e-mail to those persons who had asked for them. On occasions, a natural person who had asked for this service received an extract with personal data concerning another natural person. Subsequently the Office found that the controller had sent the account extracts as an unprotected file attached to an e-mail message and had not updated the personal data, including e-mail addresses.

International co-operation

Within the framework of building up partnerships with Central and Eastern European data protection authorities several negotiations were held:

- A two-day meeting was held with deputies of the Czech DPA in the Czech Republic in March 2006. Several topics were discussed during the meeting, including the current state of privacy protection as regards communication of public administration bodies with citizens, preparation for joining the Schengen Agreement, the performance of supervision in the SIS, and the relation between supervision bodies, inspection performance and trans-border data flow. The main result of the meeting was the approval of a joint memorandum on co-operation. Relations between the partner authorities were considered to be very good, better than the European standard, especially with regard to shared history, good language understanding and issues to be addressed.

- Two days of negotiations were held with deputies of the Croatian DPA in July 2006 in Bratislava where the main topics were the performance of supervision and inspection by the Office, as well as questions related to its organisational operation.
- Negotiations were held in Romania where the President of the Office informed partners about legislation in the field of access to public information, access to classified materials and the registration of filing systems which contain personal data.

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

On 30 November 2005, the National Assembly adopted the Information Commissioner Act[2] which entered into force on 31 December 2005. With this act the Information Commissioner was established, i.e. the two offices, the Inspectorate for Personal Data Protection and the Commissioner for Access to Public Information, were merged into a new autonomous and independent state body, and its duties and powers were defined. The Information Commissioner started work on the last day of 2005 when it assumed the tasks, competences and employees of the above-mentioned offices.

The Information Commissioner is responsible 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 there under;
- inspection supervision over 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, an extract, a list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the act governing personal data protection.,
- The Information Commissioner may file a request to the Constitutional Court 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 regarding access to public information and personal data protection).

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

The adoption of the Information Commissioner Act and establishment of the Information Commissioner ensured a full implementation of Directive 95/46/EC to the Slovenian legal order.

The Information Commissioner regularly participates in three EU working parties, which deal with personal data protection and join under the same auspices the Member States' personal data protection institutions, organised under directive 95/46/EC (Working Party 29, working parties dealing with the processing of personal data in Europol and Eurojust). Within Working Party 29, the Commissioner also has a representative in two sub-committees – ITF and SWIFT.

[1] Official Gazette of the Republic of Slovenia, No. 86/2004.

[2] Official Gazette of the Republic of Slovenia, No. 113/2005.

The Slovenian legal order implemented Directive 2002/58/EC through amendments to the Electronic Communications Act[3], adopted on 9 April 2004, and valid from 1 May 2004. Chapter 10 of this act mostly regulates the protection of personal data, privacy and confidentiality in electronic communications.

On 28 November 2006, Slovenia adopted the Act Amending the Electronic Communications Act[4], which implemented the Directive 2006/24/ES on retention of data obtained or processed in relation to providing public access to electronic communicating services or public communication networks. The act entered into force on 27 December 2006. In accordance with it, all Slovenian providers of telecommunications services (Internet access, e-mail, telephone, mobile telephone, etc.) need to retain all traffic data created through their customers' activities for a period of two years. The act's provisions regarding the retention of telephone data are scheduled to enter into force on 15 September 2007, while the provisions regarding the retention of Internet access, e-mail and voice over Internet protocol (VOIP) data are scheduled to do so on 15 March 2009.

The Information Commissioner shall also be required to carry out supervision over the execution of the Schengen Agreement, as defined in Article 128 there under, representing an independent institution's supervision of transfer of personal data for the purposes of the stated convention.

B. Major case law

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

In 2006 the Information Commissioner issued a total of nine decisions regarding the execution of biometric measures, four of which were to private legal persons and five to public legal persons, all from areas of banking, healthcare and telecommunications. Requests to grant the execution of biometric measures were in two cases sustained, in an additional two cases sustained in part, and in a further five cases refused. The Commissioner granted the use of biometric fingerprint identification for employees entering into protected areas for production and personalisation of bank and other data business cards for general use and for carrying out verification of employees entering into systems areas containing company trade secrets (records

[3] Official Gazette of the Republic of Slovenia, No. 43/2004 and 86/2004.

[4] Official Gazette of the Republic of Slovenia, No. 129/2006.

on card holders, financial transactions, card fraud cases, etc.). The Information Commissioner also issued a decision, which established that execution of biometric measures over all employees merely for the reasons of recording absence or presence at work constitutes a violation of the statutory provisions. It was established that recording of presence and absence from work is of non-vital importance for the performance of company activities, thus the execution of biometric measures would represent a disproportional and unnecessary intrusion into the employee's privacy, as recording presence in the workplace can also be achieved through less invasive methods.

Due to the established irregularities, one of the liable legal persons had to cease the use of and remove all biometric data readers previously used for employee work attendance record keeping.

In 2006 the Commissioner issued several decisions widely publicised by the national media:

1. A decision on a minor offence committed by a clothing retail company, which carried out video surveillance of working premises in its department store, specifically in the changing rooms, thus violating the provisions of the Personal Data Protection Act, which prohibits video surveillance in changing rooms, elevators and rest rooms. The supervision established that video tapes were stored, access to the video surveillance system was inadequately protected, while at the same time no traceability of data recording to removable media was ensured. The Commissioner ordered the offender to immediately cease performing video surveillance in the changing rooms, with which the latter promptly complied. Additionally, the Commissioner issued a fine as a result of breaching lawful provisions, as the offender committed a grave infringement on the privacy and dignity of people using the changing rooms in question, thus also violating their constitutional rights to personal dignity, safety and privacy.

2. A decision on the minor offence of a publishing company, which in its weekly newspaper published names of a competitive company's 86 employees receiving the highest net and gross salaries, thus illegally using, processing and presenting to the public the personal data of 86 employees, even though it had neither a statutory basis nor the individual's personal consent to process such data. The case in question entailed the processing of personal data of private sector employees, regulated in further detail by the Labour Relations Act[5].

In accordance with provisions of both the stated act and the Personal Data Protection Act, the newspaper could publish data on employee salaries only when necessary for the implementation of rights and obligations arising from employment relationships or in connection with employment relationships or with the individual's explicit consent.

The public nature of salaries has only been established[6] for the public sector, specifically stipulating that public commercial companies and commercial companies, the majority owner of which is the government (as is the case with the publishing company), do not fall into the stated public sector category.

The weekly magazine appealed to freedom of expression and public interest but, however,

[5] Official Gazette of the Republic of Slovenia, No. 42/2002, 79/2006.

[6] Zakon o sistemu plač v javnem sektorju (Official Gazette of the Republic of Slovenia, No. 56/2002).

neglected to consider the provision of paragraph 3 of Article 15 of the Constitution and Article 10 of the European Convention on Human Rights, according to which human rights and fundamental freedoms are restrained by the rights of others. Additionally, the freedom of expression was previously restrained already by the Media Act[7], stipulating that the weekly magazine would have been entitled to obtain and publish the controversial data only if such action were to prevent a grave criminal offence or immediate danger to people's lives and property, which in the present matter is not the case. The publication of data infringed on individuals' constitutional rights to personal dignity, privacy and personality rights as well as on the right to protection of personal data.

3. A decision on the minor offence of a newspaper for publishing the autopsy reports on three minors succumbing to injuries in a crush incident at a nightclub. As in the previous case the offender appealed to freedom of expression as well as to public interest. The state could not, however, be the legal basis for the processing of personal data in the private sector, especially the processing of sensitive medical personal data including data of the deceased, specifically defined in the Personal Data Protection Act's provisions. Additionally the processing of personal data was not carried out in accordance with the its original purpose. The autopsy reports were namely initially intended for use in the criminal proceedings against the nightclub owner and not for the publication in the public media.

The Information Commissioner also examined the legality of personal data processing in clinical drug-testing trials, the method of protecting patients' personal data and methods of access to such data. With regard to prior collection of an individual patient's statement in writing of consent to participate in medical trials, no irregularities were established. It was, however, uncovered that no catalogues of personal data filing systems containing data relating to clinical trials were made, additionally that no records on viewing access to medical records archives were kept, and the traceability was not ensured. During the inspection supervision, the medical institution raised a question as to the state supervisor's competency in the debated case. The latter should, according to medical experts, obtain the patient's explicit consent prior to examining any personal data. Medical experts also argued that by providing the state supervisors with requested documentation, the doctors would violate the code of medical ethics and thus endanger the doctor-patient confidentiality. For the stated reason the medical institution refused to allow review and delivery of the patients' written statements of consent and moved to stay the proceedings, in spite of the unequivocal meaning of statutory provisions (Articles 2 and 8 of the Information Commissioner Act and Articles 51 and 52 of the Personal Data Protection Act), that supervision over protection of personal data and implementation of provisions of the Personal Data Protection Act and other regulations governing protection or processing of personal data lies in the exclusive competency of the Information Commissioner as the national authority for data protection.

In order to find an amicable solution to the matter, the Ministry of Public Administration proposed that the medical documentation be inspected by a court-appointed expert. In spite of the state supervisor's full legal competency under Article 53 of PDPA to inspect the contents

[7] Official Gazette of the Republic of Slovenia, No. 110/2006.

of personal data filing systems, regardless of their confidentiality or secrecy, the Information Commissioner accepted the proposed solution.

In 2006 the Information Commissioner lodged two requests for judicial review:

1. Judicial review of paragraphs 7 and 8 of Article 128 of the Aviation Act[8], regulating the movement of persons on the premises of the public airport as well as on the premises of the air traffic control service. In the Commissioner's view the challenged provision is inconsistent with Articles 2, 15 and 38 of the Constitution and Article 8 of the European Convention on Human Rights. The Commissioner therefore moved for its annulment and, until the Constitutional Court's final judgement, the stay of its execution.

As it stands, the challenged Article severely infringes upon the individual's constitutional right to privacy of information as it anticipates collecting disproportionate amounts of personal data, a fact, both unreasonable and disproportionate with regard to the public interest and safety, both of which are essential attributes of a democratic society. The Aviation Act fails to define the purpose of collecting or processing personal data with sufficient clarity to assure the individual the necessary legal safety. In addition, the Aviation Act fails to comply with the request to state explicitly the personal data to be processed in the act itself, but rather mentions only examples of personal data to be collected.

Even though the act itself envisages the collection of personal data directly from individuals and based on their explicit consent, the establishing of such personal data filing systems should nevertheless be subject to the proportionality principle. It is namely contrary to the principle of proportionality to collect data on a period of stay, study or visit overseas, data on minor offences and pending criminal offences, issued disciplinary measures as well as type and amount of financial obligations undertaken. The request for providing sensitive personal data, which exceed their original purpose of collection (abuse of alcohol or drugs, psychological problems or illnesses), is also unconstitutional.

2. Judicial review of paragraph 1 of Article 96, paragraph 2 of Article 98, Article 100, paragraphs 5 and 6 of Article 103 and paragraph 1 of Article 114 of the Real-estate Recording Act[9], which among else regulates real-estate recording, the real-estate register, issuing of data and other real-estate related questions. The act's challenged provisions stipulate the collection of several personal data, but fail to provide a clear purpose for such a collection, leaving it inaccurate, too broad and vaguely defined. Without a statutorily defined purpose of collection it is impossible to define the type and number of personal data needed for processing.

Furthermore, the collected personal data should be implemented into the real-estate register, under Article 114 of the Real-estate Recording Act, a book of public records. The fact that statutory provisions fail to define an explicit purpose for the use of personal data shows that the act, by publishing such data, enables the use of such data for any number of possible purposes, a consequence explicitly contrary to the Constitution.

In accordance with Article 100, the real-estate register will, in addition to the data collected by estate census, be also complemented with

[8] Official Gazette of the Republic of Slovenia, No. 18/2001, 110/2002, 49/2006, 79/2006.

[9] Official Gazette of the Republic of Slovenia, No. 47/2006.

other databases. Such merging of data into a single public real-estate register is, viewed from the standpoint of privacy of information, unacceptable; that is to say, the law of personal data protection argues for a decentralised approach to personal data filing registers. With regard to the number of personal data included in the publicly available real-estate register, the Commissioner argued that the proposed solution fails to meet the principle of proportionality. It is not only disproportionate to collect excessive amounts of personal data, but also to publish them, and in addition, particularly, to merge them into a single, publicly available book of records. The publication of such data infringes on inviolability of private property as a constitutional category. There also exists a realistic threat that individuals could use such publicly available data for various, unspecified purposes, an untenable fact from a standpoint of legal safety and predictability.

C. Major specific issues

The Personal Data Protection Act specifies in considerable detail the conditions under which video surveillance of entries 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 of 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, which is to adopt a decision on video surveillance execution, publish an appropriate notice, inform its employees in writing, obtain the consent of the apartment buildings co-owners, consult the syndicates, etc. However, most of the video surveillance controllers failed to adjust their practice with the provisions of the law, which led to a large number of appeals filed with the supervisory body.

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.

At the beginning of 2006 only some 1 000 personal data controllers (there are approximately 140 000 in Slovenia) reported data on personal data filing systems which they manage. According to statutory provisions the controllers should transmit data at the latest by 1 October 2006. After this expiry, the Commissioner began issuing payment orders to liable legal persons. Thereupon some 5 500 personal data controllers

reported data to the register up to the end of 2006. The register comprises the larger part of public sector controllers, whereas a significant share of private sector personal data controllers are still not fully aware of their duties regarding the register data entries.

According to 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 supervisory body prepares and publishes opinions, explanations and instructions in relation to processing personal data in individual fields. In 2006 the Information Commissioner issued a total of 616 legal opinions.

In 2006 the state supervisors for the protection of personal data (as of April 2006, there are seven supervisors employed with the Commissioner) carried out 230 supervisions, of which 87 were in the public and 143 in the private sector.

Spain

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

The European Parliament and Council Directive 95/46/EC was enacted under Spanish Law in Organic Act 15/1999, of 13 December, on the Protection of Personal Data (LOPD)[1].

Throughout 2006, the Spanish Data Protection Agency continued to prepare the General Regulation for development of the LOPD that is now subject to official formalities at the Ministry of Justice. Its approval is expected to conclude in the first semester of 2007.

During 2006, the following regulations with an impact on data protection matters were approved:

1. Organic Act 7/2006 on the Protection of Health and combating Doping in Sport

This Organic Act specifically regulates the processing of data on doping and health in sport. Due to its effect on the fundamental right to the protection of personal data, the Spanish Data Protection Agency (AEPD) has paid special attention to ensure it contained safeguards to avoid violation of that right. The text of the law requires that data processing be limited to the purposes determined and specified, for which there is authorisation, so the information may only be used to control doping or to denounce such facts. Likewise, the duty of secrecy is also imposed on those who perform doping control duties, the access to especially protected data will be limited – establishing data dissociation techniques for certain access – and the newly created Athlete's Health Card will require high-level security measures to be adopted.

2. Act 29/2006, of 26 July, on guarantees and rational use of medicines and health products

This law regulates matters such as clinical trials with medicines, sanitary prescription or collaboration by the different public and private entities in the organisation of the rational use of medicines, with the subsequent data transferrals between them. In a report issued in 2005, the AEPD performed a series of considerations among which it emphasised the need to specify the needs and cases in which processing and cession of data arising from the electronic prescription system would not require consent by the data subject, that the publicity of the results of a clinical trial is to be performed, in all cases, following dissociation of the personal data of the subjects who underwent it and, in general, the need to adapt all data processing to the principles of the LOPD.

3. Instruction 1/2006, of 8 November, by the Spanish Data Protection Agency, on processing personal data for the purposes of surveillance using camera or video camera systems

With this instruction, the AEPD aims to adapt image processing for the purposes of surveillance to the principles of the Organic Act and guarantee the rights of persons whose images are processed by such procedures. This excludes both personal data recorded for a domestic use or purpose, as well as image processing used to exercise their duties by the security forces and corporations – processing that, in spite of being covered by specific regulations, must also fulfil the guarantees

[1] ES: https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf
EN: https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf

established in Organic Act 15/1999.The scope of this instruction includes recording, gathering, transmission, conservation and storage of images, including their reproduction or emission in real time, as well as the processing arising from the personal data related to them. Installation of cameras or video cameras will only be considered admissible when the purpose of surveillance may not be achieved by other means that, without requiring disproportionate effort, is less intrusive to personal privacy and for their right to protection of personal data. Likewise, the instruction foresees guaranteeing the right to information and provides that, in all cases, one must avoid data processing that is unnecessary for the intended purpose.

4. Act 16/2006, of 26 May, that regulates the Statute of the National Member of Eurojust and relations with the European Union

During 2006, the AEPD was also able to prepare diverse statutory instruments that affect data protection matters through the preparation of reports of a mandatory nature by its Legal Department. The following are some of the most relevant ongoing proposals:

- Bill on biomedical research
- Bill against violence, racism, xenophobia and intolerance in sport
- Bill on conservation of data on electronic communications
- Bill on conservation of police databases on identifiers obtained from DNA
- Bill on electronic administration

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

This Directive was enacted under Spanish law in Act 32/2003, of 3 November, on Telecommunications, developed by Royal Decree 424/2005, of 15 April, that regulates the conditions for the provision of electronic communications services, the universal service and protection of users.

B. Major case law

Pursuant to Article 48.2 of the Organic Act on Data Protection, the decisions by the Director put an end to the administrative channel. Due to this, and notwithstanding a remedy of appeal being lodged, those resolutions are liable to be impugned in the contentious administrative channel. In 2006, there was a total 120 sentences handed down by the National Court and five sentences by the Supreme Court resolving annulment appeals or annulment for unification of doctrine. This text only refers to the sentences in which precedents are established in controversial matters and aspects of data protection that are difficult to interpret.

- Notification of inclusion of default files

The duty to provide documentary accreditation to a data subject notifying his inclusion in a property solvency file may not give rise to penalisation of the file controller if, having followed the directives provided by the Spanish Data Protection Agency, in the sense that the notification file submitted by the company processing the default file would suffice, the agency subsequently changed criteria. That change of criteria, which considered the notification file mentioned to be insufficient, may not be applied retroactively for the purposes of penalisation.

- Electronic mail addresses are personal data

The electronic mail address held by an individual, regardless of whether or not the name address matches the name and surname of its holder, his country or the company at which he works, is personal data. This arises from the proof that it is possible to identify an individual through a simple operation, this being because the electronic mail address is linked to a specific domain and it would only be necessary to consult the server that manages that service.

- Incompatible purposes

In its sentence of April 2006, the Court found that publicity of judicial actions does not mean that the data contained in judicial proceedings which are under an enforcement phase may be examined and be available to the public at large in a completely free, indiscriminate manner, but rather that publicity is restricted, except for actions that take place at a public hearing of those holding the status of 'data subjects'. Definitively, the judicial procedures concerned may not be considered as sources accessible to the public.

- Data quality principle

The tribunal determined that the principle of data quality is required of those who submit personal data to a solvency and asset file, in the sense that they must be diligent when checking that the data reported in it is truthful. This principle begins to be breached at the moment when erroneous data is submitted to a file that provides third party information on breach of monetary obligations. It is the data controller who, at the moment of sending information to a solvency file, must be diligent over the guarantees to ensure that such solvency data as is transmitted matches the truth and, if after notification at that moment, it obtains knowledge of an error in the data, it must proceed within a reasonable time to correct and adopt the necessary measures to prevent the notice now discovered to be erroneous being formalised by inclusion.

- Especially protected data

The computer processing of data on membership of a political party is processing which is related to a person's ideology and requires his consent. Publicity of the data subject belonging to a political party, or notification to the Data Protection Agency of his appointment to public office may not be alleged as reasons to waive consent. Likewise, the possibility of penalisation arises when the data concerning ideology is used – whatever the purpose for which the person using the data acted – while it is not necessary for there to be a specific intention to reveal private data of the subject.

- Breach of the principle of consent

The use of data, although by a third party, after its holder has exercised the right to cancellation, constitutes a breach of the obligation to obtain consent. The Court determined that, although the party that uses the data is not the holder of the file delivered to it by another party, from the moment when that data is used it is submitting them to processing, which requires consent by the data subject.

C. Major specific issues

1. Transparency

- Before the Parliament

1.a) Appearance before the Parliament by the Director of the Agency

• Appearance before the Commission of the Ministry of Education and Science on the Bill on combating Doping in Sport

In June 2006, the Director of the AEPD presented Parliament with the considerations by the Agency on the Bill of the Organic Act on Protection of Health and combating Doping in Sport, with a view to its upcoming enactment proceedings. During his appearance, he emphasised that the bill, which gathered specific regulations on processing data on doping and health in sport, includes the observations made by the legal services of the LOPD, in particular, fulfilment of the principle of purpose and the duty of secrecy, on determining that the information may only be used to control doping or to report such facts, and imposing the duty to maintain secrecy upon those who perform doping control activities. Specific limitations were also established for access to especially protected data.

• Appearance before the Constitutional Commission to present the annual report for 2005

On 11 October 2006, at his own request, the Director of the Spanish Data Protection Agency appeared before the Parliament to present the annual report for 2005. In his intervention, he declared that the data contained in the annual report of the agency showed an increasingly more widespread knowledge of the 'data protection culture' in Spain, both among companies and citizens, as well as a major increase in the demand for action to be taken to ensure effective application of the guarantees foreseen in the LOPD. The Director emphasised the increase in performance of access, correction, cancellation and opposition by the citizens, a fact that shows the concern citizens have to know what information on them is recorded, and for it to be eliminated from the files. Likewise, the figures concerning the activity of the agency were broken down: these included a 40% increase in file inscription at the General Data Protection Register, a 42% increase in penalisation procedures, as well as consultation by citizens.

2. Enforcement

2.a) Telematic Notification System of the Spanish Data Protection Agency (NOTA)

In July 2006, the AEPD presented the Telematic Notification System (NOTA), the first electronic administration system offered by the body. The objective of this system, which may be used by public and private entities, is to facilitate and simplify fulfilling the obligation to notify files. The NOTA system allows three modes of file notification: by telematic means using the electronic signature; by hard copy, filled in using the NOTA system, which includes an optical reading code to expedite its inscription; and in XML format over the Internet, with or without a recognised signature certificate.

Using the agency website[2], controllers of files that contain personal data may select a file inscription form from the General Data Protection Register (RGPD), reduced from 13 to 3 pages under the new system, as follows:

[2] www.agpd.es

I. According to the controller, public or private ownership allows notification of inscription of a newly created file, as well as the amendment or suppression of a file registered at the RGPD.
II. Simplified notification or standard notification, previously filled in, allows notification of such files as customers, human resources, payrolls, owners' associations, patients, or the prescription ledger at privately owned pharmacies, or human resources files, census management, financial management, or control over access to publicly held files.
III. Standard notification is for notifying any other kind of file.

2.b) Encouragement of actions of a preventive nature: Sectorial inspections in 2006

During 2006, the AEPD has conducted ex officio sectorial inspection of non-university regulated educationals centres, in which it inspected more than 60 state and private schools in Spain. The objective of these ex officio inspections is merely preventive as, without being aimed at penalisation, it aims to make the centres audited, and in the sector it targets, aware of mandatory fulfilment of the data protection laws, it points out possible shortcomings and provides recommendations to correct these. In order to conduct this Ex Officio Sectorial Plan, pupil and family data processing by different departments and services of schools was inspected, examining such aspects as the forms used in the enrolment and place application processes, the type of data and documents gathered, the type of data contained in the academic file, data processing by the medical and orientation services at the schools, and the security measures for data protection implemented by such educational centres.

2.c) Encouraging self-regulation

- Codes of Conduct

During 2006, the following Codes of Conduct were registered at the agency, which self-regulate data protection both in public as well as private sectors.

2.c.1) Standard personal data protection code for the VERAZ-PERSUS file

The VERAZ-PERSUS is an opt-in file in which any person, himself or through his legal guardian, may request inclusion in order to avoid fraudulent use of his personal data by third parties to the detriment of his identity, solvency and financial assets. The entities using that file undertake to adopt the necessary additional measures, with criteria of diligence and confidentiality, to ensure that the person requesting the operation at its organisations is the true holder of the data included on a voluntary basis. The Standard Code establishes the conditions of the organisation and regime of operation of the VERAZ-PERSUS file, in order to offer the beneficiaries more ample guarantees than those contained in the regulations handed down on matters of personal data protection.

2.d) Investigation of reports by citizens – Special reference to the telecommunications sector

Telecommunications is the financial sector that has accumulated the largest number of denunciations during 2006, making up approximately 35% of reports and leading to several million euros in fines. This situation has taken place over recent financial years and is due to an aggressive commercial policy by diverse telecommunications operators after the process

of liberalisation of the sector, in order to achieve an increase in market share to the detriment of the former monopoly.

These practices have led some operators to register telecommunications services in the name of customers who had subscribed to those services with competing operators, which amounts to fraudulent processing of personal data without the consent of the data subject. In a high percentage of these cases, the customer refuses to pay the services registered fraudulently, causing the operator to include the customer data in default files which are shared by telecommunications companies and banks, thus blocking subscriptions to such services, which is severely detrimental to the customer.

The Spanish Data Protection Agency (AEPD) has penalised such practice for several years, causing some operators to accumulate fines exceeding a million euros in a single financial year. As a result of this, during 2006, the two main operators, which had been fined, approached the AEPD and declared their desire to comply with the data protection laws. Both operators have alleged that they proceeded to change their subscription procedures and thus put an end to the practices mentioned, offering, on a voluntary basis, to submit to an audit of the new procedures by the AEPD inspectors. Those audits were conducted at the end of 2006, and it is foreseen that during 2007 the number of such reports will begin to drop.

3. Diffusion of the data protection culture and co-operation agreements with other authorities

3.a) First European Data Protection Conference

In March 2006, the AEPD – along with the BBVA Foundation and the High Council for Chambers of Commerce, Industry and Navigation – organised the first European Data Protection Conference, in which more than 300 experts in the international political, institutional and corporate fields participated. The objective of the conference was to discuss the data protection implications in matters such as financial activity, combating terorism and organised crime, combating fraud, and administrative transparency. To that end, the conference was structured in four blocks:

I. Data protection, private sector and financial activity;
II. Data protection and security;
III. Position and meaning of the Data Protection Directive;
IV. Transparency, data protection and telecommunications.

The Binding Corporate Rules (BCRs), legal instruments in combating terrorism and their effect on privacy, identity theft, ubiquitous computing or the impact of new developments in matters of telecommunications on privacy were some of the themes debated.

3.b) Recommendations for Internet users

The implementation of Directive 2002/58/EC granted the AEPD competences to protect the rights and guarantees of users in the field of electronic communications. Within the framework of these competences and on the occasion of Internet Day in May 2006, the Spanish Data Protection Agency approved a *Recommendation guide for Internet users*. In that guide, the AEPD stated that, although new technologies are an indispensable element in the development of modern society, it is a priority to create an environment of confidence in order to use the Internet and generate a data protection

culture among citizens in the information society. The guide contains recommendations on browsing the Internet, the use of electronic mail, preventing viruses and social engineering (phishing), the use of electronic commerce and banking, or instant messenger services and chats. One must also emphasise provisions especially aimed at Internet use by minors, the use of IP telephony or file exchange through such instruments as 'Peer to peer'.

3.c) Co-operation with the Data Protection Agency of Andorra

In 2006, the Data Protection Authorities of Spain and Andorra signed a Letter of Intent to encourage co-operation between both institutions and to conduct joint actions to promote the right to data protection in both countries. In order to develop that collaboration, both authorities have committed themselves to conduct joint actions for diffusion of the rights and obligations in matters of data protection, and to provide each other with the necessary assistance to apply and interpret the data protection rules in their respective countries. They have also contemplated performance of studies, investigations or reports on the matter and co-operation with the respective governments to achieve effective guarantees in matters of personal data protection, especially with regard to international data transfers.

4. Activities by Spain on the Latin America Data Protection Network

In May 2006, the Latin American Data Protection Network met at Santa Cruz de la Sierra, Bolivia, with representatives of 12 member countries of the Latin American Data Protection Network.

During the meeting, the participants, who gathered in the four working groups created at the 4th Latin American Data Protection Conference held in Mexico 2005, on Legislation and harmonisation impulse, The on-line network, Self-regulation instruments and Processing of health data, prepared different working documents that will be submitted for approval at the next meeting of the network to be held during the first semester of 2007.

Among the main conclusions recorded in those documents, emphasis was placed on the following:

- It is necessary to adopt measures that guarantee an adequate level of protection in all the Latin American countries in order for there to be harmonisation of laws between the countries to allow the flow of information required for the correct development of the market.

- The main aim of medical records must be to provide health assistance, so that they contain all the data which require true, updated knowledge of the state of health. Access, use, filing, custody and transmission of health data contained therein require additional instruments to guarantee this and must fulfil such basic principles as respect for personal dignity, the autonomy of their will and privacy, and personal data protection. However, the basic principles of consent by the person may be limited when that limitation constitutes a necessary measure due to reasons of general interest, recognised in a regulation with a rank of law. It was also concluded that the health systems must provide guarantees of mobility, by establishing systems for health information

to be exchanged by the different bodies, centres and services of the health system, which guarantee adequate health assistance when the citizens travel around the country.

- Self-regulation initiatives, understood as a complement to the statutory framework previously defined by the state, may provide benefit in personal data protection. It is due to this that inclusion of explicit provisions tending to use self-regulation mechanisms, promotion of their publicity and establishment of effective measures to deal with breaching such rules, is recommended in the legal texts on data protection.

- Lastly, the Online Network Project was presented in order to avoid the obstacles arising from the geographic dispersion of the members of the network. The main objective of this project is to provide a virtual instrument for the Latin American network to develop and disclose its activities, diffuse the fundamental right to data protection in Latin America and configure a system to exchange information among its members.

Sweden

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

The EC Directive 95/46 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 (1998:1191) which entered into force the same day. The act applies, like the directive, to automated processing as well as manual processing. However, the rules on fundamental principles and on when processing is permitted shall not start to be applied before 1 October 2007 as regards such manual processing of personal data which 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. The directive has also been taken into account when drafting these specific acts and ordinances.

In the two preceding Annual Reports of the Article 29 Working Party (of 2004 and 2005) the report of the commission of inquiry, which was tasked with reviewing the Personal Data Act, was presented. The inquiry proposed amendments to the PDA in the form of exemptions from the handling regulations of the act. After due consideration of the proposal from the commission of inquiry, the Government (the Ministry of Justice) on 16 March 2006 presented its bill with amendments of the PDA to Parliament. In May, Parliament adopted the Government Bill implying that a 'misuse model' for processing of personal data was to be introduced as of 1 January 2007. The amendments mean exemptions from the handling regulations in the PDA. The exemptions apply to the everyday processing of personal data in unstructured material (such as the production of continuous text in word processing documents or on the Internet). The 'misuse model' applies to the processing of personal data that does not form part of and is not intended to form part of a set of personal data that has been structured in order to significantly facilitate searches for or compilations of data. For the processing of personal data that is exempted from the handling regulations one simple rule applies: processing is not permitted if it would involve improper intrusion on privacy. The handling regulations in the PDA still apply to the processing of structured data such as the processing of data in personal data registers, as well as to unstructured material that forms part of a personal data register.

The EC Directive 2002/58/EC was implemented into Swedish law by the entry into force of the Electronic Communications Act (ECA) (2003:389) in 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.

Following the adoption of the EC Directive on the retention of data processed in connection with the provision of public electronic communication services, the Swedish Minister for Justice assigned a Commission of inquiry in

May 2006 with the task of reviewing the national legislation in order to propose – in consultation with the service providers – the amendments required. The inquiry which started its work late August 2006 is expected to present a report during 2007. The Data Inspection Board is represented in the inquiry.

In last year's report the Data Inspection Board reported the fact that different commissions of inquiry during the previous few years had submitted a number of proposals aiming at facilitating the combating of crime which entailed strengthened coercive measures for the police, as well as increased possibilities to collect and register personal data. In fact more than 20 different proposals regarding control and supervision have been presented during the last two years and there has been a detailed discussion about these matters during 2006. Two bills – the Bill on enlarged use of coercive measures to prevent serious crime (2005/06:177) and the Bill on secret room wire-tapping (2005:06:178) – were submitted to Parliament in 2006 but they are dormant at the time of writing. A proposal of 2005 regarding access to electronic communication in crime investigations is scheduled to be submitted to Parliament in June 2007. In December 2006 the Government presented a draft bill implying that the signal surveillance of the National Defence Radio Establishment shall include all wire-bound traffic crossing the borders of Sweden.

In September 2006 the Commission of inquiry tasked with, among other things, reviewing the rules on patient records and healthcare, presented a proposal involving a cohesive regulation of personal data within the health and medical care services in a completely new act, the Patient Data Act. The proposal may be viewed as part of the ongoing process to establish better co-operation between the stakeholders in the health and medical care services and improve patient orientation. The proposal has been submitted to consultation and is now under consideration in the Government.

B. Major case law

In June 2005 the Data Inspection Board decided on a case regarding a co-operative economic association, the Anti-Piracy Bureau (the Bureau). The Bureau had collected scattered pieces of information, in particular Internet protocol (IP) numbers, in connection with file sharing of copyrighted material on the Internet. The Data Inspection Board had 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 therefore in breach of the provisions of that section. According to section 21 it is prohibited for parties other than the public authorities to process, *inter alia*, personal data concerning legal offences involving crime, unless the Data Inspection Board has granted an exemption from the prohibition. The Bureau claimed that the processing of personal data that was carried out was not to be regarded as processing of personal data in the meaning of the PDA. As to the IP numbers collected, the Bureau did not have access to the personal data identifying the possessor of a subscription that uses a certain IP address. However, in its decision of June 2005 the Data Inspection Board found – with reference to the preparatory work of the PDA – that the data processed in this case was to be regarded as personal data. In its decision of June 2005 the Data Inspection Board ordered the

Bureau to stop the processing, since the Bureau had not applied for an exemption from the prohibition. The Bureau appealed to the County Administrative Court of Stockholm which on 27 December 2006 rejected the appeal after which the Bureau, in January 2007, appealed to the Administrative Court of Appeal where the case is now pending.

After the Data Inspection Board's decision of June 2005 the Bureau 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 Data Inspection Board decided to grant an exemption from the prohibition of section 21 of the PDA. The exemption was to be applicable until 31 December 2006 at the latest. The Data Inspection Board has since extended the time for the application of the exemption which means that the Bureau, by virtue of the exemption at present, may process personal data relating to offences.

C. Major specific issues

Printed matter

All printed matter of the Data Inspection Board can be downloaded free of charge from the website. *Magazin DIrekt* is a quarterly periodical containing reports, news and commentaries. Certain supervisory activities are carried out in the form of specific or thematic projects and then documented in reports. During 2006 two such reports have been published: *How do debt-collecting agencies deal with complaints?* and *This is how insurance companies ought to process sensitive personal data*. The Board has also published other printed matter such as the information brochures *Information security* and *Location technology in working life*.

As to self-regulation, the Data Inspection Board has given its opinion on a final proposal for a code of conduct regarding the processing of personal data in connection with the letting of flats – a proposal of, among others, Swedish house-owners and the National Association of Tenants. In 2006, the construction industry requested an opinion from the Data Inspection Board on a proposal for a code of conduct regarding the processing of personal data within that sector. The code of conduct aims at making it more difficult with unregistered labour. Another aim is to strengthen a sound competition within the construction sector. A first meeting with representatives of this sector will be held at the beginning of 2007.

In June 2006, the Government decided on a new strategy for the development of e-Government. One of the goals of the strategy is that the government administration in 2010 will have an efficient information administration that makes information easy to access, as well as useful with due consideration to data protection and security aspects. Another goal is that sufficient sections of the government administration shall, by 2010, have become more efficient by using automated case handling systems. In 2006 the Data Inspection Board was assigned by the Government to contribute to developing efficient government administration e-services, especially concerning the legal rights of individuals as regards privacy being ensured. For this purpose the Data Inspection Board decided to make a closer study of local e-Government projects.

During 2006 the Data Inspection Board also carried out a communication exercise called 'Is your picture on the Internet?'. The purpose of this exercise was to make young people think about what a mistake on the web can lead to, as well as give guidance about what is permitted and not permitted on the web. The Data Inspection Board produced an audio programme in which a few young actors recorded five episodes on typical website problems, such as mobbing, the publication of photos and Lisa – 13 years old – who turned out to be Bengt – 53 years old. These stories were taken to a couple of youth festivals. The sound installation was placed inside the public toilets and as soon as people came in the door the soundtrack played automatically. Each story took between 60 and 90 seconds. A few more activities using the sound installation were also carried out and it is now possible to hear these stories on a special site developed by the Data Inspection Board.

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 2003.

B. Major case law

During 2006 there has been no major case law in the UK courts relevant to Directive 95/46/EC and Directive 2002/58/EC.

C. Major Specific Issues

In May the Information Commissioner laid before Parliament a special report, What Price Privacy?, on the unlawful trade in confidential personal information. This report exposed a widespread industry devoted to illegally buying and selling personal data such as addresses, ex-directory telephone numbers, criminal records and bank account details. Private investigators and tracing agents were supplying such information to journalists and financial institutions tracing debtors, among others. The Commissioner drew attention to the low penalties available for this offence and called for prison sentence of up to two years to act as a more substantial deterrent.

In December the Commissioner published his follow-up to this report, detailing the responses from government and public and private sector organisations. In this report he named the newspapers whose journalists had received personal information from one private investigator in breach of section 55 of the Data Protection Act.

In November the Information Commissioner hosted the 28th International Data Protection and Privacy Commissioners' Conference in London on the theme of the surveillance society. The Surveillance Studies Network presented a specially commissioned report "A Surveillance Society", looking at the tracking and recording of people's activities and movements now and in ten years. The conference also included contributions from a broad spectrum of speakers, representing law, government, academia, business and law enforcement. In the closed commissioners' session the CNIL presented an initiative, co-sponsored by the UK Information Commissioner and the EDPS, about "Communicating Data Protection and Making It More Effective". Alex Türk noted that rapid advancements in technology and the development of new anti-terrorism laws as challenges that data protection authorities must address.

The 2006 the Information Commissioner began a reappraisal of his approach to information sharing in the public sector. The Commissioner's guidance on the use of personal information held for collection and administration of Council Tax has been revised. It explains that we will not use our enforcement powers unless there is evidence of genuine unfairness or unwarranted detriment caused to individuals. The guidance is designed to enable local authorities to make the best use of the information they hold while protecting the interests of data subjects. We have also started work on an Information Sharing Framework Code of Practice, which will

help public sector workers in their decisions about sharing personal information. A group of information practitioners from bodies such as social services, health and police is being consulted in the production of this code.

During 2006, the Information Commissioner provided evidence to the following parliamentary select committees:

- Scottish Parliament Education Committee – Protection of Vulnerable Groups (Scotland) Bill

- Scottish Parliament Justice 2 sub-committee – Call for Evidence (Child Sex Offenders)

- House of Lords Select Committee on the European Union Sub Committee F (Home Affairs) – Inquiry into the development of the second generation of the Schengen Information System (SIS II)

During 2006, the Information Commissioner provided responses to the following consultations:

- Department for Transport – Release of Vehicle Keeper Data from the UK Vehicle Registers

- Department for Constitutional Affairs – Consultation on increase in section 55 Data Protection Act 1998 penalties.

- Driver and Vehicle Licensing Agency – Cherished Transfer and Retention Procedures

- Her Majesty's Revenue and Customs – Consultation on code of practice re Anti-terrorism, Crime and Security Act disclosures

- Home Office – Investigation of Protected Electronic Information

- Home Office – New Powers against Organised and Financial Crime

- Home Office – Consultation Regulation of Investigatory Powers Act Pt III

- Housing Corporation – Tackling Homelessness

- Information Sharing Index Project – Children Act 2004: The Information Sharing Index (England) Regulations

- **Office of Communities and Local Government** – Enabling local authorities to contract their anti-social behaviour functions to organisations managing their housing stock

- **Welsh Assembly** - 'Making the Connections' consultation on core standards of customer service for Welsh public services

Chapter Three

European Union and Community Activities

3.1. EUROPEAN COMMISSION

Commission Staff Working Document SEC (2006)95 of 20 January 2006 on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC).

This document reports on the findings regarding the evaluation of the operation of the standard contractual clauses approved by Commission Decisions 2001/497/EC[1] and 2002/16/EC[2]. The overall assessment shows that no major problems related to the use of these contractual clauses, other that the need to clarify certain aspects with a view to facilitate their use. The report also shows that Member States have little information of the use of contractual clauses. The Commission services consider that improving the monitoring by MS and data protection authorities will help to detect potential problems. The Commission services also like to see an increase in the use of standard contractual clauses as an alternative to the use of exceptions. They also point at the increasing awareness about the standard contractual clauses.

Agreement of 19 October 2006 between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security.

This Agreement, based on Articles 24 and 28 TEU replaces the previous adequacy decision and international agreement on the same matter which were annulled by the ruling by the Court of Justice of 30 May 2007 for lack of appropriate legal basis. The new Agreement relies upon the continued implementation of the Undertakings by US authorities (Department of Homeland Security, DHS and deems DHS to ensure an adequate level of protection. The Agreement provides a legal basis for the transfer of PNR data and its processing by DHS. It intended as an interim solution and should expire upon application of a superseding Agreement in principle no later than 31 July 2007.

Conference of 23-24 October 2006 on International Transfers of Personal Data, jointly with the Article 29 Data Protection Working Party -the independent EU Advisory Body on Data Protection and Privacy- and the United States Department of Commerce's International Trade Administration.

The conference was organised by the Commission in cooperation with the Working Party of the Article 29 and the US Department of Commerce. It focused on international transfers of personal data and followed the conference on "Safe Harbour" hold in Washington in 2005. The Conference devote five workshops to this topic: "Safe harbour" scheme for transfers to the US, contractual clauses, binding corporate rules, exceptions that can be invoked for international transfers in the absence of an adequate level of protection, or when specific guarantees have not been made regarding the treatment of the data and a final workshop to the question of worldwide transfers of personal data. International data protection experts, academics and representatives of private organisations from the EU and third countries control authorities took part in the Conference. The conference will have a follow up in Washington in 2007. Continuous dialogue in the field of privacy between the US and

[1] OJEU L 181, 4.7.2001, p. 19

[2] OJEU L 6, 1.2.2002, p. 52

the EU should help strengthen transatlantic relationships and to promote the emergence of a democratic information society in which the protection of personal data is ensured.

Commission Staff Working Document SEC(2006)1520 of 20 November 2006 on the application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act.

On 20 December 2001 the Commission issued the Decision 2002/2/EC pursuant to Art. 25(6) of the Directive stating that for the purposes of Art. 25(2) of the same Directive, Canada is considered as providing an adequate level of protection of personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documentation Act or PIPEDA (Canada).

The Working Document aimed at presenting pertinent findings with regard to the functioning of the Decision as well as any findings with respect to any discriminatory implementation thereof. It is mainly based on a study which was carried out for the Commission analysing the state of play in Canada as far as the application of the Decision is concerned. On the basis of the study and other information collected, the Commission services took the view that the Canadian Personal Information and Electronic Documentation Act continues to provide an adequate level of protection of personal data within the meaning of Article 25 of the Directive. The reservation formulated in Article 3 of Decision 2002/2/EC which contains safeguards necessary in case of data transfers to countries outside the European Union was maintained.

3.2. EUROPEAN COURT OF JUSTICE

Judgment of the Court (Grand Chamber) of 30 May 2006 on Passenger Name Records (Joined Cases C-317/04 and C-318/04): The court annuls the council decision concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of personal data and the Commission decision on the adequate protection of those data.

The Court notes that the decision on adequacy concerns only PNR data transferred to CBP and that the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law, which Article 3(2) of the Directive excludes from the Directive's scope. As a result, that decision does not fall within the scope of the Directive and is annulled without considering other pleas.

The Agreement relates to the same transfer of data as the decision on adequacy and therefore to data processing operations excluded from the scope of the Directive. Consequently, Article 95 EC, read in conjunction with Article 25 of the Directive does not provide a valid legal basis for concluding it. For reasons of legal certainty, the Court preserves the effect of the decision on adequacy and of the Agreement during 90 days, in order to allow for proper termination of it.

3.3. EUROPEAN DATA PROTECTION SUPERVISOR

Introduction

The European Data Protection Supervisor (EDPS) is the independent authority that ensures that the European Community's institutions and bodies[3] process personal data lawfully. The EDPS also advises them on proposals for legislation that may have an impact on data protection. Furthermore, he cooperates with the Member States' data protection authorities, as well as those in the third pillar of the European Union (police and judicial cooperation in criminal matters) to ensure consistent data protection.

These three tasks of the EDPS - supervision, consultation and cooperation - 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. The Regulation was adopted further to Article 286 of the EC Treaty. It regroups the relevant features of Directives 95/46 and 2002/58.

The EDPS started his activities in 2004. The first two years were used to literally build up the authority and to consolidate its roles. During 2006, output in terms of adopted opinions increased significantly and it was time to start assessing results in terms of compliance. A general impression is that the EU administration has improved and increasingly makes use of the EDPS to integrate data protection in their daily practice of processing personal data, as well as in the development of new legislation.

Supervision

The EDPS' supervisory role is to monitor and ensure that the Community institutions and bodies comply with their data protection obligations, as laid down in Regulation 45/2001. Because there is an urgent need to develop a data protection culture within the administration, the EDPS has allowed for a transitional learning period - until spring 2007 - after which enforcement activities will be initiated, where necessary. The major features of 2006 were:

- The number of **Data Protection Officers** (DPOs) in institutions and bodies increased throughout the year. The EDPS continued to support their network and organised a workshop for new DPOs. Bilateral evaluations of progress on notifications in large institutions take place regularly.
- In 2006, 54 **prior check opinions** were issued on risky processing systems. Of these, 49 concerned existing systems - launched before the EDPS started his activities or before the Regulation entered into force. The prior checks dealt mostly with processing of personal data relating to staff appraisal, medical files, e-monitoring, disciplinary procedures, and social services.
- 52 **complaints** were received in 2006, 10 of which were declared admissible and further examined. A large majority of the complaints received continued to fall outside of the supervisory competences of the EDPS, such as those relating to issues at national level.
- A Memorandum of Understanding with the **European Ombudsman** was signed in November, providing a framework on how to act in cases where both authorities are competent.

[3] The term 'institutions and bodies' of Regulation (EC) 45/2001 includes also Community agencies. For a full list, visit the following link: http://europa.eu/agencies/community_agencies/index_en.htm

- A number of **inquiries** were conducted in different areas during 2006. These included one on the European Commission's DG Competition, involving a large-scale sector inquiry carried out by the Commission which included collection of customer data. Another concerned the different roles of the European Central Bank (ECB) in relation to the fact that the SWIFT system (messaging network for international payments) was accessed by US authorities. The EDPS requested the ECB to ensure that European payment systems are fully compliant with European data protection laws and will follow developments during 2007.
- The EDPS also advised on more **administrative measures** than previous years. He started a survey of practices concerning personal files on own initiative. Surveys on personal data transfers to third countries and international organisations, as well as on the use of video surveillance in the institutions and bodies were also initiated by the EDPS. Work on these important dossiers will continue during 2007.
- Work has also continued within the field of the paper **'Public access to documents and data protection**. The EDPS intervened in a case before the Court of First Instance which dealt with the topic, in support of the applicants claim that the Commission should disclose the requested attendance list in full. A draft of the **e-monitoring** paper that deals with data generated by the use of electronic communications (phone, e-mail, Internet, etc.) was circulated amongst DPOs to collect comments and reactions, and a workshop was organised to test the guiding principles of the document.
- Joint work on the shared supervision of **Eurodac** continued together with the national DPAs throughout the year. The EDPS started an in-depth security audit in September 2006, in collaboration with German and French experts, and the final report will be delivered by spring 2007.

Consultation

The EDPS's consultative role is to advise the EU administration on all matters relating to the protection of personal data. This is particularly important concerning proposals for legislation that may impact on data protection. The major developments for 2006 were:

- Further development of the consultation policy and publishing an **inventory** of the intentions for 2007 on the website in December.
- The issuing of 11 formal **opinions,** covering different areas such as exchange of information under the principle of availability, visa (including access to the large scale Visa information system (VIS) for law enforcement authorities), passports and consular instructions, financial matters, as well as a second opinion on data protection in the third pillar.
- **Interventions** in external developments that relate to EDPS activities, such as the notion of interoperability, the transfer of passenger data following the PNR-judgment of the Court of Justice, retention of traffic data, the finalisation of the legal framework for the second generation of the Schengen Information System (SIS II) and negotiations in Council on the proposal for a Framework Decision on the protection of personal data in the third pillar.
- Following new **technological developments**, such as enabling technologies and R&D for

privacy and data protection. Developments in policy and legislation were also followed, not only in relation to the area of Freedom, Security and Justice, but also in other fields, such as the review of the framework for privacy and electronic communications.

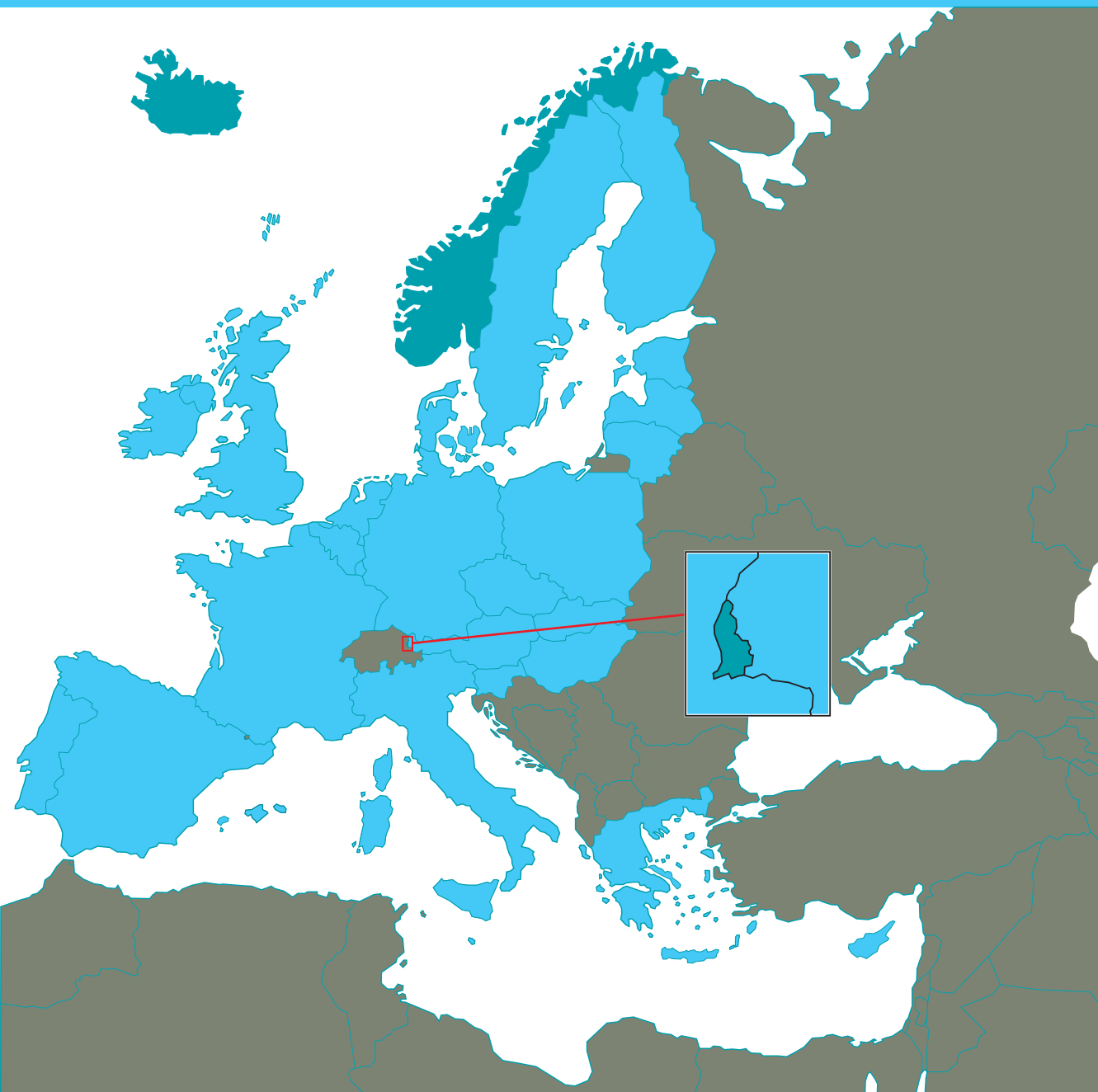
Cooperation

The EDPS's cooperative role covers not only data protection in the first pillar (EC Treaty), but also includes working together with national supervisory and supervisory bodies in the third pillar of the EU. The objective is to improve consistency in the protection of personal data and the major developments of 2006 were:

- The EDPS continued to work together closely with the **Article 29 Working Party** and actively contributed to the three opinions of the Working Party issued on airline passenger data transfers to the United States. Examples of good synergies between the opinions of the Working Party and the EDPS during 2006 were in the fields of retention of telecommunications data, maintenance obligations and the review of the e-Privacy Directive.
- Cooperation with the supervisory bodies for **Schengen, Europol, Eurojust and Customs Information System** continued to strive for high and consistent levels of data protection. Achieving this objective has become all the more urgent in light of the various proposals for exchanging personal data for law enforcement purposes.
- The EDPS also took part in the **European and International conferences** on data protection and privacy. The latter was entirely devoted to the theme "The Surveillance Society" and resulted, inter alia, in a statement that received general support and which was entitled "Communicating Data Protection and Making It More Effective" (also referred to as the London initiative). As one of the architects of the initiative, the EDPS will actively contribute to the follow-up in 2007.

Chapter Four

Principal Developments in EEA Countries



Iceland

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

In 2007, a number of acts and administrative rules concerning data protection were passed. These are the most important ones:

1. Act No. 21/2006 – Changing the Act on EEA Citizens' Freedom of Employment and Residence in Iceland, No. 47/1993, and the Act on Employment Rights of Foreigners, No. 97/2002. This act has the aim of facilitating the supervision of laws regarding employees' rights with regard to citizens from the new EU Member States, i.e. Czech Republic, Estonia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Slovakia and Slovenia. According to this act, employees from these countries shall be registered by their employers to the Directorate of Labour until 1 May 2009. Also, there are provisions on the employer's obligation to hand over documents such as employment contracts to that institution. In addition, the act allows for the linking of data on the employees in question from the Directorate of Labour, the Directorate of Foreigners, the police and the tax authorities. The Icelandic Data Protection Authority (DPA), the Persónuvernd, criticised this provision, and the Parliament decided to clarify it. It is now stated in the provision that the linking is allowed for the purpose of finding out whether the Act on Foreigners Employment Rights, No. 97/2002, is being adhered to, that linking must take place within a specified task and that their shall be no continual linking of data.

2. Act No. 46/2006 – Changing the Police Act, No. 90/2006, and the Act on the Executive Powers of the State in the Districts of Iceland, No. 92/1989. This act contains a provision which has given rise to much debate. This provision is on a so-called investigation department within the police. The debate was about whether or not this would be a secret service. However, since there are no provisions giving this department any further powers than other departments in the police, the DPA did not see a reason for making special remarks about the legal bill which became the act.

3. Act on the Obtaining of Proof on Suspected Violations of Intellectual Property Rights, No. 53/2006. This act allows for holders of intellectual property rights to obtain court rulings for the investigation of violations of such rights. Investigative actions shall always be conducted by chief legislative officials, but the holders of intellectual property have certain rights to access ceased material and to be present during investigative actions, albeit with restrictions.

4. Act on Measures against Money Laundering, No. 64/2007. This act contains provisions on the obligation of financial institutions to ask their customers to prove their identity when doing transactions and on the processing of personal data for combating money laundering. It replaces Act No. 80/1993 and is based on Directive 2005/60/EC regarding how money laundering shall be prevented and investigated.

5. Rules on Electronic Surveillance, No. 837/2006. These rules, which apply to electronic surveillance in the workplace, schools and in other areas where a limited number of people normally traverses, were passed by the Persónuvernd in accordance with Act No. 77/2000, Article 37. They replace Rules No. 888/2004 and contain provisions on, amongst other things, when

resort may be taken to electronic surveillance, for how long data recorded in the course of such surveillance may be retained, the scanning of Internet use in the workplace, automatic recording of employees' driving information, surveillance for work supervision purposes, the duty of the one responsible for surveillance to give information to the data subjects, and the obligation of the one responsible for surveillance that leads to processing of personal data, i.e. recording and to pass rules on the surveillance.

B. Major case law

On 1 June 2006, the Supreme Court delivered a judgement in a case regarding the publication of e-mails in a newspaper, i.e. whether the publication of the e-mails constituted a violation of provisions in the Icelandic Penal Code protecting privacy and whether or not an injunction against further publication of the material in the e-mails – and of the newspaper having hold of them – was lawful. The e-mails were about charges that were to be brought against prominent business men in Iceland for suspected illegal behaviour. The newspaper considered the individuals sending the e-mails between them to have started this case and that the e-mails were a proof of that. One of the individuals asked for the aforementioned injunction and filed a case against the newspaper since she considered it to have violated her privacy rights and, thereby, the aforementioned provisions in the Penal Code. The Supreme Court did not agree with that, taking into account, amongst other things, that the allegations against the business men had given rise to much public debate. Therefore, the Supreme Court argued, the e-mails were of concern for the public. In light of this, the Court put an end to the injunction and aquitted the newspaper of having been in breach of the Penal Code.

On 21 December 2006, the District Court of Reykjavik aquitted the Persónuvernd of the claim of its decision of 27 February 2006 being nullified. The case was filed by a doctor which, according to the decision, had accessed an individual's health record without permission for conducting an evaluation of his health for an insurance company. The Persónuvernd came to the conclusion that the individual in question had not consented to this access and that it was, therefore, illegal. The District Court of Reykjavik agreed with this.

C. Major specific issues

One of the main tasks that the Persónuvernd undertook in 2006 was inspections. Formal administrative decisions were taken regarding the lawfulness and security of the processing of personal data of the social services in five municipalities (including Reykjavik), three employment agencies, the Prison Office and three medical offices.

Liechtenstein

A. Transposition of Directives 95/46/EC and 2002/58/EC and further legislative developments

The following data protection laws entered into force in 2006:

The Government passed the regulation of 21 February 2006 on processing of personal data in cases of preventive protection of the state (Staatsschutz Datenschutzverordnung – StDSV) on the basis of its competence to issue regulations in accordance with Article 43 of the Data Protection Act (Datenschuzgesetz – DSG). Article 43 of the DSG establishes a series of exemptions from the provisions of the DSG for the purposes of processing personal data in specific fields related to crime prevention (terrorism, violent extremism, organised crime and illegal intelligence activities) and with a view to safeguarding state security. These exemptions remain valid until such time as further legislation governing these specific areas enters into force. The regulation was drafted in close co-operation with the data protection agency. It is crucial that relevant legislation be passed as a matter of urgency so as to re-establish equilibrium in the areas concerned with respect to the right to protection of the private sphere.

The act of 17 March 2006 governing electronic communication (Kommunikationsgesetz – KomG) entered into force. It transposes amongst others Directive 2002/58/EC.

The act on documents of domicile (Heimatschriftengesetz - HSchG) of 18 December 1985 was modified to provide for the introduction of biometric passports in line with Regulation 252/2004/EC on norms and standards for security characteristics, and biometric data in the passports and travel documents issued by the Member States. The parliamentary debate focused in particular on data safety. Article 16a of the act stipulates that these data must be included in passports. This implies that biometric data shall not be stored centrally. This is a welcome move from the point of view of data protection. The original intention was also to include the national code (PEID). However, the data protection agency provided a series of arguments against adding this number to passports, stressing in particular that, to date, it is not anchored in any legal basis. Furthermore, there were no compelling reasons for including this number in passports. In the end, the Government discarded this possibility.

Amendments were made to the legislation governing individuals and companies (Personen- und Gesellschaftsrecht – PGR) against the backdrop of Directive 2003/58/EC which sets out the disclosure requirements that fall to certain types of companies (referred to as the Updated Disclosure Directive). Essentially, the directive stipulates that all data which is subject to compulsory disclosure concerning a company must be accessible via an electronic 'record'; all documents subject to compulsory disclosure must be electronically accessible; it must be possible to correspond electronically with the registry authority, and all legal disclosures must take place and be archived by means of a central electronic platform.

In total, the DPA issued opinions on 23 bills of law.

B. Major case law

None to report.

C. Major specific issues

After the announcement in the summer that the US Finance Ministry (UST) had requested and received access to data stored in the USA with respect to international payment instructions from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), this issue was broached very rapidly by the Article 29 Working Party and in Liechtenstein itself. In this context, the DPA got in touch with the Banking Association, referring to its opinion 10/2006 on processing of personal data by SWIFT, WP 128, and in particular the obligation that falls to financial institutions to keep their customers informed. This is a complex issue and it had not yet been resolved by the end of the year.

It was not possible to complete the evaluation of implementation of the access authorisations granted within the framework of the centralised personnel register (Zentrale Personenverwaltung – ZPV) kept by the state government.[1] Some basic questions on the configuration of the system remain pending (proportionality of data processing, recording read accesses, deleting and blocking data).

Information for the public: the website of the data protection agency (www.sds.llv.li) provides information on current and/or key issues. The following are particularly worthy of note: a new training programme on data security and data protection; making telephone calls using Internet technology; spyware; hooliganism; the football World Cup and data protection; geolocation of individuals; data protection tips during vacations; document management systems (DMS), and data protection in search engines. A press release was drafted on the problem of phishing.

It is also possible to order a newsletter containing updates on data protection.

Finally, two documents entitled *Guidelines on technical and organisational measures used to guarantee data protection and Guidelines on processing of personal data by authorities* were drafted, and a special article on the topic *Consent as a central element in data protection law* was published in the Liechtenstein journal for legal practitioners (Liechtensteinischen Juristen-Zeitung – LJZ).

[1] See information already provided on this matter in the 9th annual report.

Norway

A. Implementation of Directive 95/46/EC

Significant changes to privacy or data protection law

None to report.

Significant changes to other laws affecting privacy or data protection

New Political Parties' Act
A new act relating to political parties entered into force on 1 January 2006. From a privacy protection perspective, the central provisions are those relating to the creation of a central register and the disclosure of private individuals' financial support to political parties, as well as the prohibition against accepting anonymous contributions.

One comment from the Data Inspectorate in the round of consultations was that:
'Private individuals may have quite legitimate reasons for not wanting their name to be known in connection with a donation. Our legislation should also reflect the fact that financial contributions to political parties may be a private matter.'

Whistle blowing
On 1 January 2007, new provisions entered into force relating to whistle blowing in working life. Pursuant to the new rules, business enterprises must establish solutions for whistle blowing as required but the provisions now leave the way open for anonymous notification. The routines for data, disclosure, storage, etc. follow from the Personal Data Act. The new provisions do not interfere with privacy protection in any radical way, but are mentioned nevertheless, as whistle blowing is a subject frequently discussed in the Article 29 Group.

Amendments to the act relating to child welfare services:
Due to the amendments to the Child Welfare Act, in force from 1 January 2006, employees at private crisis centres receiving operating subsidies have a duty of disclosure to the Child Welfare Authorities if they have reason to believe that children of women/men coming to a crisis centre are being neglected. The Data Inspectorate was strongly opposed to this provision and believes that it represents a serious infringement of the integrity of persons who contact a crisis centre in an emergency situation.

Act relating to the labour and welfare administration
NAV is the Norwegian Labour and Welfare Organisation. It was established on 1 July 2006 and is a comprehensive welfare reform. The NAV has an enormous amount of sensitive data on just about every person resident in Norway, from birth to death. The act led to pressure on privacy protection, hereunder on the statutory duty of confidentiality. The most problematic issue is that the number of persons with access to sensitive personal data has virtually doubled, and that no adequate access restrictions exist in the ICT system.

Regulations relating to the Armed Forces' Health Register were adopted in February 2005, but only came into force on 24 April 2006. The Armed Forces' Health Register may contain identifying personal, service and health data about defence personnel and also information about physical and social environments. The

register contains a great amount of health information about armed forces personal, without these persons having given their consent to such registration.

Amendments to the family allowance regulations
Schools may now be instructed to submit routine reports to the National Insurance Service when pupils are absent and their absence is possibly due to stays abroad. The amendments came into force in April 2006.

The Foreign Exchange Register Act came into force on 1 January 2005. In January 2006, amendments were proposed that would give the police extended access. Previously, access was only permitted in connection with investigations that had been started. Under the amended act, the criterion for access is the government agencies' need for information on their work to prevent and combat crime.

Section 7 of the Nationality Act has been given a new third section and, pursuant to this, the presentation of a police certificate is now required when applying for Norwegian nationality. The Data Inspectorate called for an assessment of whether the infringement of certain penal provisions could be considered as less relevant, but this was not followed up. The police certificate will also contain preliminary charges and indictments, even in cases where the offence has been clarified and has not been followed up by a reaction on the part of the prosecuting authorities. Fortunately, the proposal of suspending the duty of confidence of all public authorities, and at the same time subjecting them to a disclosure requirement if the immigration authorities needed information in their processing of nationality applications, was not adopted.

B. Major case law

None to report

C. Major specific issues

Traffic surveillance
The Data Inspectorate continues to work with issues regarding new surveillance infrastructures in road traffic and public transport. The inspectorate notes that some EU programmes, such as e-call, presuppose the implementation of new surveillance infrastructures. In addition to this, Norway has built fully automatic toll stations, using RFID-technology. These stations make anonymous use of certain roads and the entering of two Norwegian towns by car impossible.

Biometrics
The Data Inspectorate denied several applicants the opportunity to use biometrics in a variety of systems, reaching from a wardrobe service to access control to buildings or data systems. Five applicants complained to the Data Inspectorate's complaints commission, the Privacy Appeals Board, but only one of these complaints had been concluded by the board when this report was written. The Data Inspectorate will work further with this topic in 2007.

Insufficient protection of electronic health records
The Data Inspectorate conducted inspections at two Norwegian hospitals in 2006 in co-operation with the Norwegian Board of Health Supervision. The inspections focused on whether the health records were adequately protected. The inspections revealed an insufficient level

of information protection at both hospitals. It was pointed out that employees had wider access to health records than they needed, and that professional secrecy was thereby compromised.

Criminalisation of child grooming

In 2006, the Ministry of Justice proposed to criminalise the deliberate preparation to sexually abuse a child ('child grooming'). The Data Inspectorate asked if any new police methods were intended to follow the proposition. Searching for a person who has not made an offence, but intends to do so, can result in extensive surveillance of innocent people.

Chapter Five

Members and observers of the Article 29 Data Protection Working Party

MEMBERS OF THE ART. 29 DATA PROTECTION WP IN 2006

Austria	**Belgium**
Mrs Waltraut Kotschy Austrian Data Protection Commission (Datenschutzkommission) Ballhausplatz 1 - AT - 1014 Wien Tel: +43 1 531 15 / 2525 Fax: +43 1 531 15 / 2690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Mr Willem Debeuckelaere Privacy Protection Commission (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute, 139 - BE - 1000 Bruxelles Tel: +32 (0)2 213 85 40 Fax : +32 (0)2 213 85 65 E-mail: commission@privacycommission.be Website: http://www.privacycommission.be/
Cyprus	**Czech Republic**
Mrs Goulla Frangou Commissioner for Personal Data Protection (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 40, Themistokli Dervi str. Natassa Court, 3rd floor - CY - 1066 Nicosia (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 Office for Personal Data Protection (Ú ad pro ochranu osobních údaj) Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tel: +420 234 665 111 Fax: +420 234 665 501 E-mail: posta@uoou.cz Website: http://www.uoou.cz/
Denmark	**Estonia**
Mrs Janni Christoffersen Danish Data Protection Agency (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tel: +45 3319 3200 Fax: +45 3319 3218 E-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk	Mr Urmas Kukk Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) Väike - Ameerika 19 - EE - 10129 Tallinn Tel: +372 6274 135 Fax: +372 6274 137 E-mail: info@dp.gov.ee Website: http://www.dp.gov.ee
Finland	**France**
Mr Reijo Aarnio Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki (P.O. Box 315) Tel: +358 10 36 66700 Fax: +358 10 36 66735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi	Mr Georges de La Loyère French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés - CNIL) Rue Vivienne, 8 - CS 30223 FR - 75083 Paris Cedex 02 Tel: +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**
Mr Peter Schaar **Chairman** The Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) Husarenstraße 30 - DE - 53117 Bonn Tel: +49 (0)1888 7799-0 Fax: +49 (0)1888 7799-550 E-mail: poststelle@bfdi.bund.de Website: http://www.bfdi.bund.de Mr. Alexander Dix (representing the German States / Bundesländer) The Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit) An der Urania 4-10 - DE - 10787 Berlin Tel: +49 30 13 889 0 Fax: +49 30 215 50 50 E-mail: mailbox@datenschutz-berlin.de Website: http://www.datenschutz-berlin.de	Mr Nikolaos Frangakis Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Ampelokipi - GR - Athens Tel: +30 210 6475600 Fax: +30 210 6475628 E-mail: contact@dpa.gr Website: http://www.dpa.gr
Hungary	**Ireland**
Mr Attila Peterfalvi Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary (Adatvédelmi Biztos) Nador u. 22 - HU - 1051 Budapest Tel: +36 1 475 7186 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Website: http://www.abiweb.obh.hu	Mr Billy Hawkes Data Protection Commissioner (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE - Co.Laois Tel: +353 57 868 4800 Fax: +353 57 868 4757 E-mail: info@dataprotection.ie Website: http://www.dataprotection.ie
Italy	**Latvia**
Mr Francesco Pizzetti Italian Data Protection Authority (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Roma Tel: +39 06 69677 1 Fax: +39 06 69677 785 E-mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it	Mrs Signe Plumina Data State Inspection (Datu valsts inspekcija) Kr. Barona 5-4, Riga, LV - 1050 Tel: +371 6722 31 31 Fax: +371 6722 35 56 E-mail: signe.plumina@dvi.gov.lv, info@dvi.gov.lv Website: http://www.dvi.gov.lv

Lithuania	**Luxembourg**
Mr Algirdas Kunčinas State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) Žygimantų str. 11-6a - LT-01102 Vilnius Tel: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-mail: ada@ada.lt Website: http://www.ada.lt	Mr Gérard Lommel National Commission for Data Protection (Commission nationale pour la Protection des Données - CNPD) 41, avenue de la Gare - LU - 1611 Luxembourg Tel: +352 26 10 60 -1 Fax: +352 26 10 60 – 29 E-mail: info@cnpd.lu Website: http://www.cnpd.lu
Malta	**The Netherlands**
Mr Paul Mifsud Cremona Office of the Data Protection Commissioner 2, Airways House High Street - MT - SLM 1549 Sliema Tel: +356 2328 7100 Fax: +356 23287198 E-mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt	Mr Jacob Kohnstamm Dutch Data Protection Authority (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10 - NL - 2595 CL The Hague (Postbus 93374 - 2509 AJ The Hague) Tel: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl
Poland	**Portugal**
Mr Michał Serzycki Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw Tel: +48 22 860 70 86 Fax: +48 22 860 70 90 E-mail: kancelaria@giodo.gov.pl Website: http://www.giodo.gov.pl	Mr Luís Novais Lingnau da Silveira National Commission of Data Protection (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lisboa 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 Office for the Personal Data Protection of the SR (Úrad na ochranu osobných údajov SR) Odborárske námestie 3 - SK - 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441 E-mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	Mrs Natasa Pirc Musar Information Commissioner (Informacijski pooblaščenec) 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.ip-rs.si
Spain	**Sweden**
Mr Artemi Rallo Lombarte Spanish Data Protection Agency (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES - 28001 Madrid Tel: +34 91 399 6219/20 Fax: +34 91 445 56 99 E-mail: director@agpd.es Website: http://www.agpd.es	Mr Göran Gräslund Data Inspection Board (Datainspektionen) Fleminggatan, 14 (Box 8114) - SE - 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se Website: http://www.datainspektionen.se
United Kingdom	**European Data Protection Supervisor**
Mr Richard Thomas Information Commissioner's Office Wycliffe House Water Lane,SK9 5AF Wilmslow GB Tel: +44 1625 545745 Fax: +44 1625 524510 E-mail: please us the online enquiry from our website Website: http://www.ico.gov.uk	Mr Peter Hustinx European Data Protection Supervisor - EDPS 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 2006

Iceland	**Norway**
Mrs Sigrun Johannesdottir Data Protection Authority (Persónuvernd) Raudararstigur 10 - IS - 105 Reykjavik Tel: +354 510 9600 Fax: +354 510 9606 E-mail: postur@personuvernd.is Website: http://www.personuvernd.is	Mr Georg Apenes Data Inspectorate (Datatilsynet) P.O.Box 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**
Mr Philipp Mittelberger Data Protection Commissioner (Stabsstelle für Datenschutz -SDS) Kirchstrasse 8, Postfach 684 - LI - 9490 Vaduz Tel: +423 236 6090 Fax: +423 236 6099 E-mail: info@sds.llv.li Website: http://www.sds.llv.li	Mr Krassimir Dimitrov Commission for Personal Data Protection –CPDP (Комисията за защита на личните данни) 1 Dondukov - BG - 1000 Sofia Tel: +359 2 940 2046 Fax: +359 2 940 3640 E-mail: kzld@government.bg Website: http://www.cdpd.bg
Romania	
Mrs Georgeta Basarabescu National Supervisory Authority for Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, 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
Mr Alain Brun Head of unit European Commission Directorate-General Justice, Freedom and Security Data Protection Unit Office: LX46 01/43 - BE - 1049 Brussels Tel: +32 2 296 53 81 Fax: +32 2 299 8094 E-mail: Alain.Brun@ec.europa.eu Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

NE-AC-08-001-EN-C
DOI 10.2758/12429

EUROPEAN
COMMISSION

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 978-92-79-08173-6