Eleventh Annual Report

of the Article 29 Working Party on

Data Protection

EUROPEAN COMMISSION

1830-6446

Eleventh Annual Report

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

Covering the year 2007

Adopted on 24 June 2008

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 http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

TABLE OF CONTENTS

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

Technological and economic developments lead to more and more comprehensive data processing in increasingly complex IT systems. At the same time, intensified co-operation between EU Member States contributes significantly to cross-border processing of personal data, for example in connection with the EU Services Directive.

Furthermore, initiatives launched by the Council or the Commission aimed at improving the fight against terrorism and crime have an impact on the processing of personal data in the Internal Market. For example, if – in accordance with Directive 2006/24/EC – telecommunications and Internet service providers are required to retain traffic data for later use or if air carriers are obliged to transfer passenger data which they collect and store for providing their own services.

Therefore, it is little wonder that in 2007 European Data Protection Authorities also had to deal with numerous challenges, but also accomplished major tasks. Thus, the Article 29 Working Party adopted 17 opinions. Moreover, the Working Party elaborated and published other documents on important data protection related issues.

Of particular importance was the highly debated processing of passenger data collected by air carriers for law enforcement purposes. The Article 29 Working Party took a very critical stance on the negotiations about an EU-US PNR Agreement and was also outspoken when, in November 2007, the Commission presented its own model aimed at introducing a similar PNR regime within the EU.

The Article 29 Working Party made an important contribution to the interpretation of the concept of "personal data" within the meaning of Directive 95/46/EC. It addressed the arduous but vital topic of Binding Corporate Rules (BCRs) in order to speed up the coordination procedure among data protection authorities, and following lengthy debates it convinced the SWIFT company, which was criticised because of the access of US authorities to data on international money transfer, to change its data processing method and data transfers by setting up a new operational centre in Europe.

Some key areas are set out below:

A major activity of the Article 29 Working Party in the year covered by this report was the 1st Data Protection Day held on January 28, the anniversary of the adoption of the European Convention 108 by the Council of Europe in 1981.

Jointly proclaimed by the EU data protection authorities and the Council of Europe, numerous activities were launched together with parliamentarians, politicians and NGOs across Europe. Informing European citizens, raising awareness among youngsters and exploring the challenges for an effective protection of privacy were at the heart of all those endeavours. Open doors, panel discussions, meetings with high ranking government officials and wide media coverage underlined the importance of data protection in the light of the latest EU proposals and industry initiatives threatening the privacy of our citizens.

A thorough evaluation of all activities related to the European Data Protection Day aimed at exchanging experiences among data protection authorities and showing best practices will help to perform even better in 2008 and the years ahead.

By elaborating and adopting an opinion on personal data (**WP 136**), the Article 29 Working Party has made an important contribution to the uniform interpretation and harmonised application of a key concept of Directive 95/46/EC. Different interpretation of the notion of personal data could endanger legal certainty and hamper the free flow of data. The paper intended as guidance to all those dealing with the collection and processing of personal data has to be considered a milestone in the work of the Article 29 Working Party and will serve in many future discussions concerning the possibility of using and re-identifying anonymised data.

In July 2007, the third EU-US PNR Agreement was signed following a rather intense, but constructive debate with the Commission and the Council on the basic principles of the agreement and a well attended workshop jointly organised with the European Parliament's LIBE Committee in March 2007.

In their **WP 138** adopted on 17 August 2007, the Working Party welcomed the fact that the new long-term agreement provides for a legal basis for the transfer of passenger data thus avoiding a legal lacuna, but they voiced their explicit criticism concerning the level of data protection foreseen in the deal as being too low. As the new agreement leaves open many questions, the Article 29 Working Party has turned to both the Commission and the Council with the hope of clarifying at least these issues.

As to the EU PNR proposal presented by the Commission on 6 November 2007, the Article 29 Working Party could not but express their deep disappointment (**WP 145**). The proposal is too closely modelled on the previously signed EU-US PNR Agreement. The Commission could – from the perspective of data protection agencies - not substantiate any pressing need for such a new, additional system in particular in the light of Directive 2004/82/EC (API Directive) which already mandates airlines to collect data contained in the passengers' passports and which can - apart from border and immigration controls - be used for law enforcement purposes as well. The Article 29 Working Party maintains that, regardless of numerous shortcomings and flaws in the proposal that have to be reconsidered, first of all a thorough evaluation of the API-Directive should be conducted to see whether passenger data are indeed a useful tool in the fight against terrorism and serious crime.

The Article 29 Working Party called, therefore, on the Council to enter into a dialogue with all those agencies and companies involved in the collection and processing of traveller data, in particular with airlines, operators of computer reservation systems, the European Parliament, both data protection and consumer protection organisations to find privacy enhancing solutions which are acceptable to all stakeholders and take account of their legitimate concerns.

Of great importance, too, was the adoption of **WP 130** regarding the processing of personal data in electronic health records held by hospitals, doctors and health authorities. Given the importance of this sector and due to the fact that in particular sensitive data are collected and processed, the Article 29 Working Party found it vitally important to raise awareness and give guidance to all those working in that field. Following the publication of the paper in a so-called "consultation procedure" the Article 29 Working Party received numerous comments which shall be debated and possibly considered in the year 2008.

The Article 29 Working Party concluded the joint enforcement action of data protection authorities of Member States in the health insurance sector by publishing a final report on its website. For the first time all EU data protection authorities jointly and systematically worked together in investigating and examining an industry sector which concerns almost all EU citizens and which collects and processes huge amounts of personal data which to a large extent are sensitive ones. Given the outcome of the investigation, the Article 29 WP will carry on monitoring the implementation of Directive 95/46/EC in other sectors in the years to come.

On 15 and 16 October 2007 – this time organised by the US Department of Commerce and the Federal Trade Commission – the 3rd Safe Harbor Conference took place in Washington. The conference stressed the importance which the Article 29 Working Party, the Commission and the participating US authorities attribute to EU-US relations in the field of data protection. The participants considered it crucial that, in view of an ever increasing exchange of persons and goods between the two continents, such a dialogue is to be continued and intensified. In view of the increasing challenges, the changing political and technological developments have to be taken into account. All participants confirmed that the Safe Harbor Conference was an appropriate forum to achieve a better understanding of each other's data protection system and to establish common legal and real bases for guaranteeing effective protection of personal data.

In addition, the Article 29 Working Party also agreed on a procedure to speed up the approval procedures for binding rules on the dealing with personal data in internationally operating companies and corporations (Binding Corporate Rules (BCRs)). Despite some progress in that field, much needs to be done to improve the current coordination among supervisory authorities. Therefore, the Article 29 Working Party will intensify the dialogue with industry with a view to achieving further optimisation of the procedures.

Furthermore, at the request of the Commission the Article 29 Working Party adopted opinions on the EU's Internal Market Information System (**WP 140**) and the Consumer Protection System (**WP 139**). The issues raised in the papers will be of great interest for the future work of the Working Party.

All in all, the year 2007, too, was globally marked by a tendency that governmental agencies and companies increasingly encroach on the private life of citizens. It does not seem likely that this tendency will decrease, even in the years to come. Therefore, it is vital that society is aware of these threats and is reacting in an appropriate manner. Also in the future, the Article 29 Working Party will make every effort to contribute to guaranteeing citizens' basic rights to data protection.

This is the last activity report I will present as Chairman of the Article 29 Working Party, because my second tenure will end in February 2008. Therefore, I would like to thank all colleagues who have contributed to the results of our common work. In particular, I would like to mention Prof. José Luis Piñar Mañas, who, from February 2004 to February 2007 represented the Article 29 Working Party as Vice Chairman, and Alex Türk, the President of the CNIL, who assumed this task in April 2007. I would like to thank in particular the Secretariat under Alain Brun, the Head of Unit, which has excellently supported our work and I would like to thank all staff members of the national data protection authorities, who in the background have contributed to the success of our work.

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/2007_en.htm

1.1. TRANSFER OF DATA TO THIRD COUNTRIES

1.1.1. Passenger Data/PNR

Opinion 2/2007(WP 132) on information to passengers about transfer of PNR data to US authorities

This opinion and its annexes (frequently asked questions and model notices) are aimed at travel agents, airlines, and any other organisations providing travel services to passengers flying to and from the United States of America. They update and replace the previous opinion of 30 September 2004 (WP97). The current legal framework for transferring PNR information to the US authorities is covered by the interim agreement of 16 October 2006. Negotiations for a new agreement[2] are expected to start in 2007. This opinion aims to give advice and guidance on who needs to provide what information, how and when. Information should be provided to passengers when they agree to buy a flight ticket, and when they receive confirmation of this ticket. The opinion gives advice on providing information by phone, in person and on the internet.

The Article 29 Working Party has established the model information notices (the annexes to this opinion) to make providing this information easier for organisations, and to make sure the information provided is consistent across the European Union.

Opinion 5/2007(WP 138) on the follow-up agreement 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 concluded in July 2007

This opinion aims to analyse the impact on fundamental rights and freedoms and in particular the passengers' right to privacy of the new and third agreement on the transfer of passenger name record (PNR) data to the US Department of Homeland Security (DHS). The fact that a new long-term agreement has been reached provides for a legal basis for the transfer of passenger data. The Working Party has always supported the fight against international terrorism and international organised crime, and considers it necessary and legitimate. However, any limitation of the fundamental rights and freedoms of individuals, including the right to privacy and data protection, has to be well justified and has to strike the right balance between demands for the protection of public safety and other public interests, such as the privacy rights of individuals.

Joint Opinion (WP 145) on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007

This opinion aims to analyse the impact on fundamental rights and freedoms, in particular passengers' rights to privacy, of the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes presented by the European Commission on 6 November 2007. The proposal is closely modelled on the EU-US PNR agreement signed in July 2007 and many features of the present draft are similar to that agreement. The privacy concerns raised by the Article 29 Working Party on that PNR agreement therefore remain valid for a couple of points expressed in this opinion. The opinion also takes into account the findings of the Article 29 Working Party's opinion 9/2006 of 27 September 2006 on Directive 2004/82/EC of the Council as that Directive also foresees the transfer of passenger data by air carriers to government authorities. In the case of a European PNR regime the limitation of fundamental rights and freedoms has to be well justified and has to strike the right balance between demands for the protection of public security and the restriction of privacy rights.

1.1.2. Binding Corporate Rules (BCR)

Recommendation 1/2007 (WP 133) on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data

The Data Protection Directive 95/46/EC allows personal data to be transferred outside the EEA only when the

[2] In Brussels on 23 July 2007 and in Washington on 26 July 2007 a new agreement was signed between the European Union and the United States of America. Council Decision 2007/551/CFSP/JHA of 23 July 2007, OJ L 204 of 4.8.2007, p.16 Agreement between the European Union and the United States of America, OJ L 204 of 4.8.2007, p.18 http://europa.eu.int/eur-lex/lex/JOHtml.do?year=2007&serie=L&textfield2=204&Submit=Search&_submit=Search&ihmlang=en

third country provides an "adequate level of protection" for the data (Art. 25) or when the controller adduces adequate safeguards with respect to the protection of privacy (Art. 26). Binding Corporate Rules (BCRs) are one of the ways in which such adequate safeguards (Art. 26) may be demonstrated "by a group of companies in respect of intra group transfers"[3] although the BCRs are not a tool expressly listed and set forth in the Data Protection Directive 95/46/EC. The use of BCRs to provide a legal basis for international data transfers from the EEA requires the approval of each of the EEA data protection authorities (DPAs) from whose country the data are to be transferred.

1.1.3. Jersey

Opinion 8/2007 (WP 141) on the level of protection of personal data in Jersey

The Channel Islands consist of five main islands: Jersey, Guernsey, Alderney, Herm and Sark, located in the English Channel within the Gulf of St Malo off the north-west coast of France. Constitutionally, they are divided into the Bailiwicks of Guernsey and Jersey. The Bailiwick of Jersey is a dependency of the United Kingdom. The United Kingdom is responsible for Jersey's international affairs and for its defence. Jersey itself has autonomy in relation to its domestic affairs, including data protection. Jersey is part of the customs territory of the Community. The common customs tariff, levies and other agricultural import measures apply to trade between Jersey and non-Member countries, and there is free movement of goods in trade between Jersey and the Community. However, other Community Rules, including those relating to data protection, do not apply. When the United Kingdom transposed the Directive, Jersey's authorities indicated that such legislation would not apply to Jersey. Since then, it has introduced its own data protection legislation. Pursuant to Article 299 of the Treaty establishing the European Community, the Directive does not apply to Jersey and so it is a third country within the meaning of Articles 25 and 26 of the Directive.

1.1.4. Faroe Islands

Opinion 9/2007 (WP 142) on the level of protection of personal data in the Faroe Islands

The Faroe Islands are located in the North Atlantic. They are comprised of 18 islands. The islands are administratively divided into seven counties, which are divided into 120 communities. Together with Denmark and Greenland, the Faroe Islands constitute the Kingdom of Denmark, which is a constitutional monarchy. Under the 1948 Home Rule Act the islands became a self-governing community within the Kingdom of Denmark. The Home Rule Act divides all policy areas into two main groups, whereas common affairs are under Kingdom authority and Special (Faroese) Affairs are under Faroese Home Rule administration and legislation. The regulation of personal data in the Faroe Islands is based on laws passed by the Faroese Parliament and on laws regulating common affairs. The Data Protection Act (DP Act) was passed by the Faroese Parliament in 2001, and is administered by the Faroese Data Protection Agency (DPA).

The Danish Data Protection (DP) Act applies only to the data processing of Kingdom authorities (i.e. the police, and the prosecution, the county jail and the prison and probation service, the High Commissioner of the Faroe Islands, processing of cases in the area of family law, church authorities). Since the Danish DP Act[4] is based on the Directive, it is assumed that it provides at least adequate protection with regard to the processing of personal data, and accordingly those areas are not considered herein.

1.2. ELECTRONIC COMMUNICATIONS, INTERNET AND NEW TECHNOLOGIES

Opinion 1/2007(WP 129) on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities

[3] See Working Document WP 74, Section 3.1: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

[4] Act No 429 of 31 May 2000 on Processing of Personal Data. This Act implements Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The European Commission has adopted its Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities (COM (2006) 474) on 1 September 2006 (the "Green Paper"). The aim of the Green Paper is to stimulate the discussion in the area of detection technologies at the European level and gather *"thought-provoking answers and concrete suggestions"* towards *"strengthening the common approach towards detection technologies"* to be construed in the *"broadest sense"*. The Article 29 Working Party, along with other parties, was invited to participate in the consultation process.

The replies to the questions raised in the Green Paper as well as other comments made will determine concrete steps and actions that could be subsequently taken. Furthermore, depending on priorities identified in the course of the public consultation, specific steps could be taken as soon as possible. If stakeholders show their interest, a task force delivering actions on specific subjects could be created. Such a task force could consist of representatives from various Members States authorities and experts from the private sector.

1.3. ACCOUNTING, AUDITING AND FINANCIAL MATTERS

8th Directive on Statutory Audits, Opinion (WP 143) 10/2007 by the Article 29 Working Party

On 15 February 2007, the Article 29 Working Party examined a working document presented by DG Internal Market on transfers to third country public regulators of audit working papers containing personal data. The working paper explains the EU legal regulatory framework set up by Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts (the 8th Directive). The 8th Directive provides for the conditions to carry out the statutory auditing activity and sets out an independent public oversight for statutory auditors by Member States. It also contains specific provisions relating to the cooperation between public oversight bodies from Member States and competent authorities of third countries. Such co-operation should include the exchange, with third country authorities, of the auditor's working papers and other documents held by European audit firms.

1.4. PERSONAL DATA

Opinion 4/2007 (WP 136) on the concept of personal data

The Working Party is aware of the need to conduct a deep analysis of the concept of personal data. Information about current practice in EU Member States suggests that there is some uncertainty and some diversity in practice among Member States as to important aspects of this concept which may affect the proper functioning of the existing data protection framework in different contexts. The outcome of this analysis of a central element for the application and interpretation of data protection rules is bound to have a profound impact on a number of important issues, and will be particularly relevant for topics such as Identity Management in the context of e-Government and e-Health, as well as in the RFID context.

The objective of the present opinion of the Working Party is to come to a common understanding of the concept of personal data, the situations in which national data protection legislation should be applied, and the way it should be applied. Working on a common definition of the notion of personal data is tantamount to defining what falls inside or outside the scope of data protection rules. A corollary of this work is to provide guidance on the way national data protection rules should be applied to certain categories of situations occurring Europe-wide, thus contributing to the uniform application of such norms, which is a core function of the Article 29 Working Party.

1.5. BIOMETRICS & HEALTH DATA

Working document (WP 131) on the processing of personal data relating to health in electronic health records (EHR)

In this Working Document on the processing of personal data relating to health in electronic health records

(EHR), the Article 29 Working Party provides guidance on the interpretation of the applicable data protection legal framework for EHR systems and explains some of the general principles. The Working Document also gives indications on the data protection requirements for setting up EHR systems, as well as the applicable safeguards.

The Article 29 Working Party first examines the general legal data protection framework for EHR systems. The Article 29 Working Party recalls the general prohibition of the processing of personal data concerning health of Article 8(1) of the Data Protection Directive 95/46/EC, and then discusses the possible application of the derogations in Article 8(2), (3) and (4) of the Directive in the context of EHR systems by stressing the need for interpreting such derogations in a narrow fashion. The Article 29 Working Party also reflects on a suitable legal framework for EHR systems and provides recommendations on eleven topics where special safeguards within EHR systems seem particularly necessary in order to guarantee the data protection rights of patients and individuals.

Opinion No 3/2007 (WP 134) on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications (COM(2006) 269 final).

The current proposal for an amendment to the CCI is designed to create the legal basis for the mandatory collection of biometric identifiers from visa applicants and to establish provisions on the organisation of Members States' consular offices – in the light of the common visa policy and the enhanced integration between consular offices. The adoption of a Regulation amending the Common Consular Instructions on visas in relation to the introduction of biometrics is a "precondition" for the implementation of the Visa Information System (VIS)[5] since it provides "a legal framework for the collection of the required biometric identifiers".

The Visa Information System will be set up and regulated upon entry into force of the Regulation of the European Parliament and the Council concerning the VIS and the exchange of data between Member States on short-stay visas, which is under discussion. The establishment of a centralised database containing data on visa applicants, including fingerprints and digitised facial images, together with data on group travellers and people providing hospitality in the applicants' countries of destination, is said to be one of the keys to implementing a common visa policy and to achieving the objectives set out in Article 61 of the Treaty on the European Community (TEC), namely the free movement of persons in an area of liberty, security and justice.

1.6. ENFORCEMENT

Report 1/2007 (WP 137) on the first joint enforcement action: evaluation and future steps

In its First report on the implementation of the Data Protection Directive (COM (2003) 265 final), the European Commission called upon the Article 29 Working Party (WP 29) *"to hold periodic discussions on the overall question of better enforcement… and consider the launching of sectoral investigations at EU level and the approximation of standards in this regard"* with the objective of understanding the level of implementation and providing guidance to sectors, improving compliance in the least burdensome ways possible.

In response, the Working Party mandated the Enforcement Task Force (ETF) in June 2004 to discuss an EU strategy and criteria for enforcement. In November 2004, in its Declaration on Enforcement (WP 101), Article 29 WP announced its commitment *"to developing proactive enforcement strategies [and] increasing enforcement actions"* and identified six criteria to consider in identifying a sector for collaborative enforcement.

The combination of the criteria identified in WP 101 pointed to the selection of a sector with highly harmonised activity and furthermore, whose impact on

[5] Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (COM(2004) 835 final) presented by the Commission on 28 December 2004.

the protection of personal data would be equally high. Article 29 WP therefore selected private medical insurance as the object of this first synchronised intervention, specifically in the provision of health assistance insurance.

1.7. CONSUMERS

Opinion 6/2007 (WP 139) on data protection issues related to the Consumer Protection Cooperation System (CPCS)

This Article 29 Data Protection Working Party (Working Party) Opinion discusses the data protection issues related to the Consumer Protection Cooperation System (CPCS), an electronic database operated by the European Commission for the exchange of information among consumer protection authorities in Member States and the Commission pursuant to the provisions of Regulation (EC) No 2006/2004 on consumer protection cooperation (CPC Regulation).

The Opinion follows a letter dated 30 March 2007 by the head of Unit B-5, Enforcement and Consumer Redress, of the European Commission's Health & Consumer Protection Directorate-General (DG SANCO) addressed to the Secretariat of the Working Party and requesting the opinion of the Working Party.

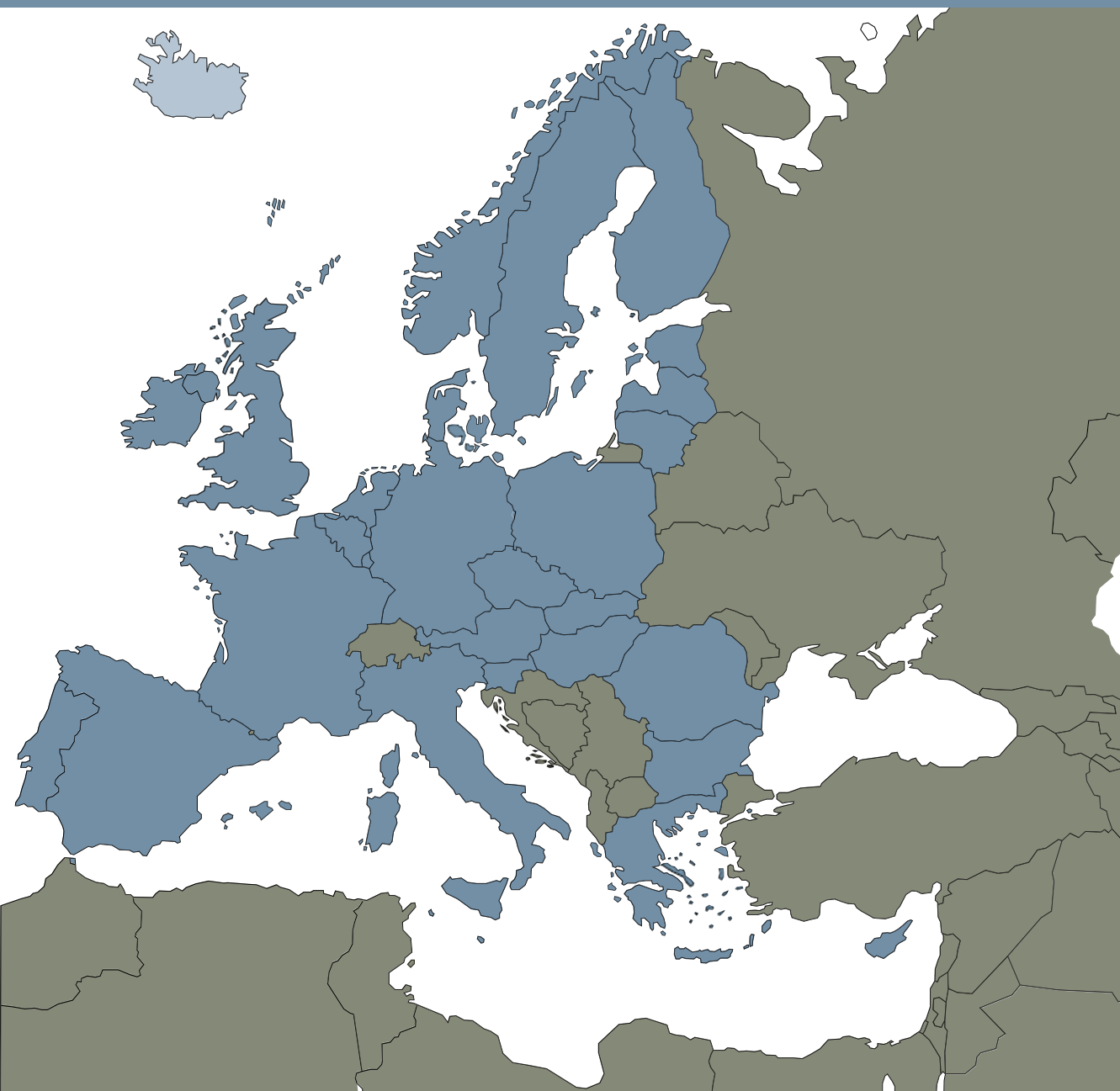
1.8. INTERNAL MARKET INFORMATION SYSTEM (IMI)

Opinion 7/2007 (WP 140) on data protection issues related to the Internal Market Information System (IMI)

The project of setting up a computerised system as a tool for exchange of information concerning personal data raises important concerns with respect to the fundamental rights of individuals, in particular the right to privacy.

The complexity of the Internal Market Information System (IMI) and the diverse issues it involves led DG Internal Market of the European Commission to request the opinion of the Article 29 Working Party (WP 29). The WP 29 Opinion will focus on the same issues addressed in the documents "Issue paper on Data Protection in IMI" (D-4784) and "General Overview" (D-1804). The objective of this opinion, then, is to analyse the implications IMI creates with respect to personal data, protected by Directive 95/46/EC (Data Protection Directive) and Regulation (EC) No 45/2001 (Data Protection Regulation).

Chapter Two
Main Developments in Member States



Austria

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

The Data Retention Directive 2006/24/EC has not been implemented yet. A draft was sent out in spring 2007, but met with considerable criticism. The Data Protection Commission, which was supposed to serve in a supervisory role, also submitted a negative comment on the draft. No new draft has been sent out since.

B. Major case law

A citizen wanted to know from his Austrian bank what of his personal data had been handed over to US authorities by SWIFT. The Data Protection Commission rejected the complaint he had raised when the bank did not give the desired response, ruling that SWIFT had acted independently and was itself responsible for providing this information (Case number K121.245/0009-DSK/2007).

A patient had a disagreement with a doctor about the kind of treatment required. The doctor wrote a brief note describing the incident, which included a remark about the patient's emotional state, which the patient found inappropriate. He demanded that this remark be removed based on the right of rectification. The hospital (as the data controller) refused, and the Data Protection Commission dismissed the complaint, ruling that the information was correct insofar as it represented the doctor's account and personal impression of the incident (Case number K121.246/0008-DSK/2007).

An Austrian citizen committed a traffic violation in Switzerland. The Austrian authorities helped their Swiss counterpart to identify him by transmitting personal data. The citizen brought a complaint before the Data Protection Commission, which was dismissed. He challenged the decision before the Austrian administrative court (*Verwaltungsgerichtshof*, abbrev. VwGH). His arguments included the claim that the Data Protection Commission lacked the independence required by Article 28 of Directive 95/46/EC. The administrative court dismissed all of his arguments and confirmed that the Data Protection Commission was organised in accordance with relevant EC law (Decision VwGH Zl. 2006/06/0322).

For case law on video surveillance, see the entry under "Major specific issues".

C. Major specific issues

Video Surveillance
Issues regarding video surveillance remain high on the agenda of the Data Protection Commission. In 2007, the Commission granted permission in several cases. One case involved video surveillance on the subway network of the Vienna Public Transport Company (Wiener Linien GmbH & Co KG). The company wanted video surveillance as a measure against vandalism and to protect employees and passengers. The Commission issued a limited permit which will expire on 30 June 2009. After this deadline, the Vienna Public Transport Company must show the positive effect of video surveillance before the permit is renewed.

There has been considerable discussion about this and notification of video surveillance in large apartment blocks.

The issue of video surveillance has received increased coverage in the media, as well as much attention from citizens.

Credit Reporting
In recent years, the Austrian cellular telephone providers, among other companies, have adopted the practice of checking the creditworthiness of every new customer. This has led to a large number of complaints by citizens whose application was rejected following a negative report. The Data Protection Commission has addressed a number of issues in this context. The conduct of the credit reporting agencies towards data subjects who exercise their rights of access, rectification and deletion was often found to be unsatisfactory. The accuracy of data was another issue that needed to be addressed.

One credit reporting agency claimed that it was not the data controller for a portion of the evaluation process on the grounds that the companies that ordered these reports merely took the raw data and fed it into a scoring

system under their own control. The Data Protection Commission ruled that this was indeed true and that the companies themselves were data controllers for this part of the system. The Commission decision has been challenged before the Austrian Constitutional Court (*Verfassungsgerichtshof*).

Moreover, the Data Protection Commission has taken steps to establish firm rules for credit reporting databases, especially a large database called the "consumer credit registry" (*Konsumentenkreditevidenz*).

Belgium

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

On the 15th anniversary of the *Act of 8 December 1992 on the Protection of Privacy with regard to the Processing of Personal Data* (hereafter referred to as the Act on Privacy) which transposes Directive 95/46/EC into national law, the Commission for the Protection of Privacy (hereafter referred to as the Belgian Commission or the Commission) prepared an *annotated version*[6] of this legislation. This commentary provides a number of references – normative and jurisprudential – for each of the articles of the law considered useful to ensure the clear understanding and interpretation of these provisions and to put them into context. The European statutory texts (of both the European Union and the Council of Europe), the opinions of the Article 29 Working Party, the jurisprudence of the European Court of Human Rights are among the sources referred to in particular in this reference guide. This anniversary also provided the Belgian Commission with the opportunity to assess 15 years of its work and the prospects and challenges ahead, and to debate some current issues at an academic session held at the Parliament.

Act on Electronic Communications
During 2007, the Belgian Commission examined a proposal to amend the *Act of 13 June 2005 on Electronic Communications (Opinion 18/2007 of 27 April 2007*), which transposes Directive 2002/58/EC into Belgian law (*Belgian Monitor,* 20 June 2005). While this proposal did not ultimately succeed, the amendments that it put forward are nevertheless worthy of mention since they aimed to improve the protection of privacy within the scope of the provision of mobile telephone location services. On one hand, it proposed providing users of the system with the same guarantees regarding the protection of their privacy as subscribers (mandatory prior user notification, mandatory notification of activation of the service directly to the mobile telephone with each location request and the right to cancel the services for the end user), and, on the other, extending this protection to minors from the age of 12 (obtaining their consent in addition to that of their legal representatives). However, the act of 13 June 2005 was not amended in the sense described above.

Act governing the installation and usage of surveillance cameras
The previous Annual Report stated that the issue of video surveillance was of great concern to both the legislator and the Belgian Commission in 2006.

After lengthy discussions and a series of hearings with parties concerned by the issue – including the Belgian Commission – the *Act governing the Installation and Usage of Surveillance Cameras* was adopted on 1 March 2007 (hereafter referred to as the Cameras Act, *Belgian Monitor* 31 May 2007). This sectoral legislation specifically governs the processing of images for surveillance purposes. However, with the exception of explicit exemptions, the act remains in force. The main elements of this new regulation can be summarised as follows:

The Cameras Act applies to all permanent or mobile observation systems installed and used for the surveillance and monitoring of certain areas. The installation and usage of surveillance cameras governed by specific legislation (private detectives, security at football matches) as well as the installation and usage of cameras to ensure health and safety, the protection of a company's goods, or to monitor the production and work processes at the workplace, are excluded from its scope.

The Cameras Act distinguishes between three types of area (open areas, closed areas accessible to the public and closed areas not accessible to the public), each of which is subject to specific regulations with regard to the procedure for installation of the surveillance camera and to its usage.

Only the placement of a surveillance camera in an open area is subject to obtaining prior favourable opinion from local political officials and a favourable opinion from the local police service, confirming that a security and efficiency study has been carried out and that the planned system adheres to the principles of data protection regulations. The assessment of proportionality will differ depending on whether the camera is placed

[6] This document is available as a CD-ROM from the Commission. It can also be downloaded from its website.

in one area or another (images filmed, access to data, data recipients, retention of data, number of systems). For example, the cameras must be placed on public roads to prevent private areas (such as entrances to, or windows of, private buildings) from being included in their scope. Also with regard to open areas, real time viewing is only permitted under the supervision of the administrative or judicial authorities with the aim of enabling the police to intervene directly in the event of an offence, damage or breach of public order.

In order to meet its notification obligation, the party responsible for the processing must put up a sign indicating the existence of camera surveillance. Any hidden usage of cameras is prohibited (cf. *Opinion 22/2007 of 13 June 2007 on the preliminary draft of the royal decree defining the means of indicating the existence of camera surveillance in compliance with the Act of 21 March 2007 governing the Installation and Usage of Surveillance Cameras*).

Irrespective of the area in which the party responsible for processing wishes to install a surveillance camera, they must notify the Belgian Commission of their decision using a form specially produced for this purpose (specific thematic declaration). Furthermore, the local police service must be simultaneously notified of any installation of cameras in a closed area.

Set-up of sectoral committees
Sectoral committees set up within the Belgian Commission verify that the processing of personal data carried out in various specific sectors (social security, public authorities etc.) does not infringe upon privacy. Some of these committees are responsible for the authorisation of certain kinds of processing. These committees are made up, on the one hand, of members of the Belgian Commission, and on the other, of experts appointed for their practical knowledge of the sector concerned. Several of these joint committees started their work in 2007 and requests for authorisation addressed to them are on the increase.

Communication of healthcare data
The 2006 Annual Report stated that a draft act on the creation of a sectoral social security and healthcare committee was to be adopted at the beginning of 2007. Under the *Act of 15 January 1990 on the Establishment and Organisation of a Central Social Security Database* amended on 1 March 2007, the responsibilities held by the sectoral committee for social security until that time were extended to include certain processing of personal healthcare data. The new healthcare section of this committee is therefore responsible for authorising the communication of healthcare data in so far as this communication is legally required. It is also responsible for ensuring adherence to provisions established by or pursuant to the Act on the Protection of Privacy with regard to the processing of such data.

B. Major case law

No decision of particular importance made by the courts is considered worthy of mention.

C. Major specific issues

General introduction
The trend to centralise and interconnect data, already noted in 2005 and 2006, was confirmed in 2007. In its opinions issued during this year, the Belgian Commission has, as in previous years, focused on the necessary respect for the principle of compatibility between files, in order to avoid the systematic crossing of data, and on the necessary transparency of this processing with regard to citizens, and the retention of a certain degree of control over information by everyone. The increase in the number of electronic administration projects (cf. public sector) provided the opportunity for the Commission to reaffirm these principles.

Though not all of them have been successful, some legislative initiatives are also worthy of mention, as they aimed to provide a clear legal framework for the processing of particularly sensitive data, such as that requested for inclusion in the national police database, or for the processing of data which is required more and more frequently, such as taxation data. This also provided the Belgian Commission with the opportunity to underline some key principles.

As in 2006, the Belgian Commission carried out verification of adherence to data protection legislation by the company SWIFT. It also checked adherence to legislation

by companies concerning the establishment of internal alert systems (whistle-blowing) and to the transfer of personal data abroad (for example, through the adoption of binding corporate rules).

Finally, the Belgian Commission also drew up positions and recommendations concerning new technologies, such as digital television and other interactive media, as well as the distribution of images, in general, and, in particular, in the school environment.

The various facets of the Belgian Commission's activities in 2007 are set out below.

Police and security sector

National police database: in its opinion 12/2007 of 21 March 2007, the Belgian Commission welcomed the regulatory initiative aiming to establish the conditions under which the police services may collect and process personal data and information within the scope of their mandate. It examined this proposal in light of the requirements – of predictability and proportionality in particular – of the European Convention on Human Rights (ECHR) and of the jurisprudence of the court responsible for overseeing its application. The Commission, however, made its favourable opinion subject to conditions, finding, on several points, that the proposal only summarily met the requirements of Article 8 of the ECHR. While stating its awareness of the practical difficulty of structuring and categorising all of the raw information collected or sent to the police services, it found it necessary, in particular, to define these information systems as precisely as possible to enable citizens to reasonably foresee what information is likely to be included and for what reasons.

Public sector

Data processing by the financial administration: the Belgian Commission also examined the initiative aiming to regulate the processing of certain personal data carried out by both the financial administration – and its various departments – and within the scope of the external relations that this administration maintains with other public and private organisations. The draft text put before it aimed, firstly, to bring current practices in financial administration into line with the Act on Privacy, and, secondly, to establish a legal framework for both the overall, integrated computerisation of financial administration and the usage, within the scope of combating tax evasion, of automated tools to assist decision-making. The following, in particular, were provided for: (1) the creation of a "single file" record for each taxpayer (natural and/or legal person); (2) the processing of data using an automated tool to assist decision-making (*data warehouse*) to identify risks and groups at risk with regard to the complete or partial non-adherence to taxation legislation (data mining); and (3) data flows leaving and entering the Federal Public Financial Service, sent to or received from other authorities and professions.

In the opinions issued on this initiative, the Belgian Commission highlighted the following points in particular *(Opinion 01/2007 of 17 January 2007 and 16/2007 of 11 April 2007 on the preliminary draft of the act on the processing of personal data by the Federal Public Financial Service)*:

- Any exchange of data collected for different purposes – also within the same financial administration – cannot be presumed compatible, but has to be subject to the compatibility analysis provided for by Article 4 of the Act on Privacy before implementation. This provision explicitly sets out that data cannot be subsequently processed in a way that is incompatible with the purposes for which it was originally collected, taking into account relevant factors, in particular reasonable provisions of interested parties and legal provisions. An internal authorisation procedure following examination by an *ad hoc* committee cannot act as a substitute;
- The Commission approves of the distinction made between administrative management tasks and those of controlling, recovery and litigation. In this respect, it specifies that the description of these purposes should be based on functional criteria and not on organic criteria;
- Even though taxation data is not classified as "sensitive data" *sensu stricto* under Belgian legislation, it is often rightfully considered as such, as its impact on everyone's privacy is so significant;
- The Commission is of the opinion that such specific regulation must – in principle – adhere to the Act on Privacy. If, for certain reasons, exemptions to the basic regulations on the protection of personal data should prove necessary and justified, these exemptions must be included in the Act on Privacy itself;

- While the Commission has no objection to the creation and use of a sectoral taxation identification number, it has reservations about the use of this taxation identification number in the financial administration's external relations and the risk that such a number would become, *de facto,* a second universal identification number. The general use of this taxation identification number should not replace the use of the national registration number established in Belgian law by a committee responsible for ensuring, through its powers of authorisation, it is used in adherence to the Act on Privacy;
- The Commission is not opposed to the setting up of internal controls within an organisation or public service. On the contrary, it welcomes the creation of an internal committee responsible for ensuring "internal compliance" with data protection legislation, without prejudice to its own responsibility for external controlling, and to that of its sectoral committees;
- With regard to the duration and conditions of data retention, the Commission requires regular evaluation of the necessity to retain data and the retention conditions. It recommends regular, mandatory evaluation of the necessity to retain this data before the expiry of the maximum deadline. The data should be deleted as soon as it is no longer considered accurate, relevant or necessary. The Commission also recommended that a clear distinction is made, following each evaluation, between data required for current activities and that which, if necessary, is to be archived;
- Finally, the Commission welcomes the specific procedural framework for the use of the *data warehouse* and data mining techniques provided for by the draft act, since this framework provides guarantees to ensure that these tools are not used opaquely and disproportionately. Before all decoding or insertion of additional data into the *data warehouse*, a report, which carries out a balance of interests and necessity analysis, will be submitted for review to the internal control committee. In addition to this procedural framework, the Commission recommended that an *ad hoc* department (trusted third party) be set up with responsibility for decoding and coding the data. However, this regulatory proposal was not successful.

Automated decisions: within the scope of the opinions issued in response to this, and other, regulatory proposals, the Commission emphasised the necessity of adherence to the prohibition of decision-making based only on automated data processing that could result in legal consequences for specific persons, or could affect specific persons in a significant way. Whether it concerns a decision aiming to provide an automatic benefit for the person concerned – for example, measures simplifying administration – or a decision that is part of a controlling procedure or to combat fraud, the Commission invariably remains vigilant. Even where authorised by law, such decision-making should be accompanied by appropriate guarantees aimed at maintaining a certain degree of control over the information by the person concerned.

Within the scope of its evaluation of the specific regulatory proposal concerning data processing by the financial administration mentioned above, the Commission contends that the data processing and decision-making – such as a decision to instigate a tax inspection of a certain person – cannot be carried out exclusively on the basis of information provided by the *data warehouse*.

In its opinion on a proposal to automatically apply the maximum price for the supply of electricity and natural gas to customers on modest incomes – based on the coupling of the data of energy providers and social security data – the Commission pointed to the existence of this prohibition and the necessity of adherence to the principle of proportionality, and suggested the implementation of an opting-out system.

Coupling – intermediate organisation: the requests for authorisation of the transfer of data flows addressed to the Belgian Commission and its sectoral committees also show that, with the aim of administrative simplification, but also sometimes as part of a controlling procedure, various public authorities are increasingly seeking to couple (as in the example above seeking the automatic setting of a preferential tariff) the data of the same citizen. In this area, the most frequently sought data is, for example, data concerning the financial situation of the person concerned for the granting of any right or benefit that is determined by income. This increased recourse to coupling has led the Belgian Commission to advocate the intervention of an intermediate organisation (*trusted*

third party), providing all the guarantees of independence required to ensure the genuine confidence of the persons concerned (cf. *The opinion 02/2007 of 17 January 2007 on the draft royal decree governing the regulations according to which certain hospital data is to be communicated to the Minister responsible for public health*).

Subsequent processing for statistical and scientific purposes: the role of an intermediate organisation with regard to subsequent processing of data for historical, statistical or scientific purposes was also specified. When dealing with a request from a researcher for access to cadastral data available within the financial administration, the Commission specified what guarantees should be provided by academics when processing personal data for statistical and scientific purposes (*Opinion 32/2007 of 7 November 2007 on the use of cadastral data for the purpose of statistical and scientific research).* On this occasion, it also referred to its jurisprudence - and that of its sectoral committees - over the use of the single national identification number. In order to balance the interests of researchers to collect personal data for the purposes of scientific or statistical research and those of citizens to control the use made of their data, the Commission recommends a working method whereby the person responsible for the processing of the database, from which the sample of persons to question is taken, contacts the persons concerned to ask for their consent to be included in the study planned (*Opinion 16/2006 of 14 June 2006 on the conditions governing the communication of data from the national records for (scientific) research*).

Private sector

Swift: the processing of personal data carried out by the company SWIFT, and in particular its transfer to the United States and the consultation of this data by the United States Treasury (UST) with the acknowledged aim of combating terrorism, was, in 2006, the subject of two opinions from the Belgian Commission. The Commission pronounced the violation of several provisions – criminal offences – of the Act on Privacy by the Belgian company in its capacity as the party responsible for data processing. Throughout 2007, the Commission closely followed the development of this issue and the measures implemented by SWIFT to bring its activities into line with Belgian regulations. In this respect, it embarked on a recommendation procedure in relation to this company. At the time of going to press, this procedure was still ongoing.

Binding Corporate Rules – BCR: the Act on Privacy confers the mandate on the King, in line with the opinion of the Belgian Commission, to authorise the international transfer of data to a third country deemed inadequate on the basis of binding corporate rules, by providing sufficient guarantees in terms of data protection. The company General Electric (GE) chose this framework with regard to its cross-border data flows concerning its employees. In accordance with its rules, GE undertakes to notify the Federal Public Justice Service (Ministry of Justice) and the Belgian Commission if a foreign legal obligation requires the communication of data, except where this authority specifically prohibits this information. While the Commission welcomes this notification obligation – advocated by the Article 29 Working Party, in accordance with its WP 128, on the processing of data carried out by SWIFT referred to above -, it is of the opinion (1) that the exemption concerned should be limited to the prohibition issued by the sole authorities responsible for ensuring adherence to the law, (2) this prohibition must have a legal basis and (3) that it must be limited in time. Furthermore, the Commission's positive opinion depends on the removal of the exemption to the right to opposition based on the individual consent of the employee and the insertion of the possibility for an audit by the data protection authorities. (*Opinion no 13/2007 of 21 March 2007 on the draft royal decree authorising transfers to a country that is not a member of the European Community and that does not ensure an adequate level of personal data protection for the employees of General Electric*).

Whistle blowing: the 2006 report stated that following numerous questions and requests concerning the introduction of professional ethical guidelines within enterprises (whistle blowing), the Belgian Commission adopted a *recommendation on the compatibility of professional alert systems with the Act on Privacy.* Based on this recommendation, in 2007 the Belgian Commission welcomed a professional alert system set up by the Flemish ombudsman authorised to carry out inquiries concerning the denunciation of irregularities by members of staff of the Flemish public services.

New technologies

Digital television: in an opinion on the digital transmission of traditional television services, excluding other possibilities made available by digital television (for example, interactivity), the Commission made the following observations:

- The automated processing of digital television data by cable companies should be qualified as the "processing of personal data";
- With regard to the legitimacy of the processing, the Commission found that to support the collection of personal data, the digital television cable company could invoke either the consent of the person concerned or the necessity of carrying out such processing, for example for invoicing purposes, in the execution of the distribution contract signed by the data subject. However, the Commission excludes any prevalence of the legitimate interest of the cable company with regard to the protection of the privacy of the consumer concerned (Article 5 f) of the Act on Privacy – (Article 7f) of the Directive 95/46/EC);
- The opinion emphasises, in particular, the importance of the principle of purpose and the effectiveness of the rights of the person concerned;
- Finally, the Belgian Commission welcomes the adoption of a code of conduct specifically aimed at this sector.

(Opinion 06/2007 of 7 February 2007 on digital television and the protection of privacy)

Interactive means of media consumption: in an opinion 29/2007 of 19 September 2007, focusing on new means of media consumption in general, the Belgian Commission highlights new privacy risks posed by new means of media consumption, especially if they are interactive, and with particular regard to interactive television: user profiling, manipulation of users, loss of the right to anonymous consumption of media and loss of the right to information, cultural diversity and media pluralism. With regard to profiling, the opinion emphasises that the supply of the service and profiling constitute two distinct objectives. (Subsequent) processing of data for the purposes of profiling is therefore only permitted if the person concerned has clearly consented to it. It should be verified that the freedom of consent has been respected: a refusal of profiling may not result in the withdrawal of the service, and more generally, the blocking of these new means of media consumption.

Recommendation concerning the distribution of images

In general: in view of the increase in the distribution of images on increasingly numerous and varied platforms, the Belgian Commission has seen fit to issue a recommendation on the matter. Interested parties should refer to this (*initiative recommendation 02/2007 of 28 November 2007 on the distribution of images).*

In the school environment: based on the principles established, the Belgian Commission expressed an opinion on the distribution of photographs of minors in the school environment. Such distribution is in fact on the increase, whether through the posting of class photographs on the school's website or by means of the publication of individual photographs. The Commission pointed out that the principles of the Act on Privacy apply without restriction to the processing of this personal data. It excludes the applicability of exemptions provided for the processing of data for journalistic purposes.

In principle, the consent of the persons concerned is required for the processing of this personal data. In the case of minors without the power of judgement, this consent is to be obtained from their legal representatives. In the case of minors with the power of judgement, the Commission recommends involving the minor by asking for his/her own consent *and* that of his/her legal representatives.

The Commission also distinguishes between specific and non-specific photographs. Tacit consent may be presumed when taking a *non-specific photograph* aimed at reporting a given event (group photograph at a school fête, publication in a school journal). The persons concerned nevertheless have to be informed of the taking of the photographs, their purpose and the type of publication envisaged. The use of such photographs for school publicity purposes is excluded. Such photographs must not be detrimental to a person's good reputation. No additional personal data should accompany the photograph. This precaution should be observed in particular where sensitive data is revealed.

For *specific photographs* (individual portrait, for example), the informed consent – in particular with regard to the exercise of the rights of information access, rectification

and opposition – of the person concerned is required for each type of image taken and method of distribution. Applying the principle of proportionality, the Belgian Commission also recommends that, if the purpose of publication on the Internet is to inform parents and pupils, the publication should be part of a website where access is reserved for these groups, for example through the introduction of a password.

New website of the Belgian Commission for the Protection of Privacy

On the first European Data Protection Day, the Belgian Commission launched its new website, which has greatly improved content compared to the previous version. This site is designed to meet both the requirements of citizens seeking information and the need to make the public aware of personal data protection. All the opinions, recommendations and authorisations referred to here are available at the following website http://www.privacycommission.be.

Bulgaria

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

The full implementation of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995, on the protection of individuals with regard to processing personal data and the free movement of such data in Bulgarian legislation, was accomplished by the amendments of the Law on Personal Data Protection (LPDP) in 2006.

Directive 2002/58/EC of the European Parliament and the Council of 16 September 2002 on processing personal data and protection of privacy in the electronic communication sector was implemented by the Electronic Communication Act promulgated in the State Gazette, issue 41 of 2007.

In 2007 Ordinance No 1 of 2007 on the minimum level of technical and organisational measures and the permitted type of personal data protection, issued in compliance with Art. 23, para. 5 of LPDP was adopted and promulgated in the State Gazette, issue 25 of 2007. By virtue of the Ordinance, the minimum level of technical and organisational measures in processing personal data and the permitted type of protection are determined.

New Regulations on the Activity of the Commission for Personal Data Protection (CPDP), in compliance with Art. 9, para. 2 of LPDP, were promulgated in the State Gazette, issue 25 of 2007. The regulations govern the issues, functions and activity of CPDP, and the legal regulation aims at the strict implementation of LPDP and also at establishing clear rules for personal data controllers and data subjects.

B. Major case law

In 2007 typical cases of violation of Directive 95/46/EC, as well as of LPDP, relate to illegal processing of personal data of individuals without their consent and without advance notification by the data controllers about the processed categories of personal data, as well as about the purposes for which they are processed, the recipients of their personal data and the right of individuals to access their personal data.

CPDP handled complaints concerning personal data processing which exceeded the specific, strictly determined legal purposes, as well as further processing in a way that was not in line with these purposes. These cases show illegal data retention with a view to using data for other purposes, including direct marketing. In CPDP's experience, it can be concluded that individuals are particularly sensitive regarding the disclosure of certain categories of their personal data, mostly related to their health, but these were not typical cases in 2007.

2007 saw a considerable decrease in the number of complaints relating to personal data processing for direct marketing purposes or video surveillance, without the awareness and consent of individuals.

With regard to the dissemination of personal data on the Internet, the work of CPDP shows that in most cases personal data are collected by means of registration on websites, and the individuals provide such data of their own accord.

In 2007, CPDP expressed opinions concerning issues relating to the legal processing of personal data by personal data controllers. Requests for opinions were made both by personal data controllers and by individuals with regard to their rights under LPDP. Opinions were expressed regarding legal processing of personal identity numbers (PIN), personal data processing for statistical purposes, prerequisites for legal processing of personal data of customers of companies providing public services, as well as photocopying identity cards of clients of banks.

Following the amendments to LPDP in 2006 and the adoption of the new Art. 36a of LPDP, the Commission made decisions both regarding personal data transfer to the countries of the European Union and to third countries. In cases when personal data controllers transfer personal data to other data controllers in the territory of third countries, outside the European Union and European Economic Area, CPDP made a decision after making an assessment concerning an adequate level of personal data protection ensured in the third country. This assessment is made in accordance with criteria such as the nature of data provided; the duration of data processing; the purpose of providing personal

data; notification of individuals whose data is provided concerning the purposes of provision and the recipients of the data in the third country; right of access of the individual and the opportunity for rectification or deletion where processing is not in compliance with LPDP; provided for data protection in the third country, and measures providing for the opportunity of compensation for damages suffered by the individual as a result of illegal processing. In 2007, the requests of personal data controllers addressed to CPDP in compliance with Art. 36a of LPDP, relate to the provision of personal data of appointed employees under employment contract to the data controllers with the sole ownership of the capital of separate companies located in third countries in compliance with Art. 1, item 14 of the Additional Provisions of LPDP. Requests were also made by data controllers whose activity includes selection of staff and hiring sailors for sailing under a foreign flag.

C. Major specific issues

In January 2007, the implementation of a twinning project BG/2005/IB/OT/02 under PHARE program BG2005/017-586.03.01 started: Further Strengthening the Administrative Capacity of the Bulgarian Commission for Personal Data Protection and Providing Conditions for Implementation of the Law on Personal Data Protection.

The twinning project was divided into five components: 1: analysis of the legislative framework; 2: institutional building; 3: information system of CPDP; 4: complaints handling and inspections; 5: strategies and methods for raising the public awareness of the activity of CPDP.

The project included 42 activities which comprise its main objective – institutional building and investment related to it in Bulgarian CPDP, in order to achieve higher efficiency and better operation of activities concerning personal data protection in the country through the adoption and implementation of the best practices of the EU in prevention of violations in personal data protection, as well as for their best protection.

The activities included different fields of personal data protection: telecommunications, Ministry of Interior, justice, health, insurance, direct marketing, banks, video surveillance, e-government, etc.

The implementation of activities provided for in the twining project was accomplished in February 2008.

PHARE program BG2005/017-586.03.01 provides for the implementation of a delivery contract. The contract is expected to be signed by the end of February.

Each month, monitoring reports on the project, ensuring safeguards and effective control, are carried out.

In 2007 a web-based information system for registration of personal data controllers with the following opportunities was developed:

1. Filling in the application form in a special section of the website of CPDP – www.cpdp.bg;
2. Confirmation for the completed data with and without the use of an electronic signature;
3. Registration of the approved personal data controllers (PDC) in CPDP register "Register of PDC and the registers kept by them" with a unique identification code;
4. The register is public, and the access to it is provided by the website of CPDP – www.cpdp.bg;
5. Receipt, on the e-mail of the registered RDC, of official confirmation that they are registered in the system, as well as the user's name and password for access to their own profile, with which they can perform updates on changes that have occurred in the declared circumstances;
6. Accessibility of data from the public register, both for the registered PDC and for all interested parties that can be informed at any time on the new activities and on the new status of the organisations.

At present, the system is in the last stage of tests and operates within the local network of CPDP. It is expected to be accessible for all PDC through the website of CPDP in the first months of 2008 – www.cpdp.bg.

Republic of Cyprus

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

Directives 95/46/EC and 2002/58/EC:
No new developments to report.

On 31 December 2007, a law entitled "The Retention of Telecommunications Data to be used for the Investigation of Serious Criminal Offences" was published in the Official Gazette of the Republic.

This law transposed the provisions of Directive 2006/24/EC of 15 March 1966 on the retention of data generated.

The period for the retention of data has been fixed for six months.

Serious criminal offences have been defined as offences that are a felony according to the Criminal Code or any other law or which carry a maximum sentence of five years imprisonment or more.

Access to telecommunications data retained under the law is permitted only after an order of a President of a District Court or a Senior District Judge after an application for such access is made by a police investigator with the approval of the Attorney General.

There is express provision that the retention or discovery of the content of the communication is prohibited.
Telecommunications data which have been given to the appropriate authority by virtue of a Court order must be destroyed within a period of 10 days from the date when the Attorney General of the Republic considers that they are not connected with the commission of a serious crime.

In order cases the data shall be destroyed in accordance with a policy prescribed by the Chief of Police and approved by the Supervisory Authority.

The Commissioner for the Protection of Personal Data has been designated as the Supervisory Authority for the purpose of supervising the implementation of the law.

The Supervisory Authority has power to conduct audits and examine complaints and to submit a case to the Attorney General of the Republic where a violation may constitute a criminal offence.

In accordance with a declaration made by the Republic of Cyprus, the provisions of the law relating to the retention of communications data relating to internet access, internet telephony and internet e-mail shall come into force on 15 March 2009.

B. Major case law

After a publication in a daily newspaper in March 2007 which referred to the situation prevailing at the old Nicosia General Hospital (after its relocation to a new building), the Commissioner decided to carry out an investigation.

The investigation revealed that documents were left in certain parts of the old hospital which contained personal data of patients and that, despite the presence of security guards at the entrance to the hospital, access to the premises was uncontrolled and anybody could also access the buildings and any documents found therein, including people who were carrying out repairs at the hospital.

Explanations were given by representatives of the Ministry of Health which was responsible for the relocation of the hospital regarding the security measures and the data that was left at the old premises.

Thereafter measures were taken to prevent unauthorised entrance to the premises and the documents found therein were taken to a safe place and/or destroyed.
Taking into account all the circumstances of the case and the fact that there was compliance with the directions of the Commissioner, a fine of Cyprus £1500 was imposed on the Director-General of the Ministry.

A spam case involving the sending of unsolicited communications to mobile phones relating to horse racing results was investigated after a number of complaints were submitted to the Commissioner. The messages were sent (by several numbers) using prepaid telephone cards. The sender of these messages never

responded to our letters or answered our questions and after following the prescribed procedure, the Commissioner proceeded to issue a decision imposing a fine of Cyprus £2000.

C. Major specific issues

An audit was carried out at the Land Registry Department in order to ascertain the way the department carried out its various processing operations.
The audit was carried out on the basis of a questionnaire and it was found that:

- Information given to data subjects relating to the processing of their data was not sufficient/satisfactory;
- The department collected information from third parties and did not inform the data subjects accordingly;
- Data relating to owners of immovable property were given to municipal and other local authorities for the purpose of imposing land taxes without informing the owners about this;
- In certain documents used by the department, excessive and irrelevant information is being collected;
- The personnel of the department who are engaged in processing personal data have not received any information/training in respect of the Data Protection Law nor had they received any written or other guidance relating to their duties and obligations.

The findings of the audit were communicated to the department and we are monitoring the steps they are taking to comply with the instructions of the Commissioner.

Employees of a local authority complained to the Commissioner about the fact that they were required to have their fingerprints taken for the purpose of checking their arrival and departure from work.

During the examination of the complaint, the local authority concerned stated that they decided to use this method because the method used before (the punching of a card) was abused (the employees destroyed their cards or would punch other employee's cards) and they found that this method was more effective and could not be abused. The authority also demonstrated to the Commissioner the specific system used for the taking of the fingerprints. After taking into account all arguments and information put before him, the Commissioner decided that, in the circumstances, the taking of the fingerprints for the purpose of checking the attendance of employees was not lawful and asked the authority to stop this practice and destroy all fingerprints already collected.

As there were also other complaints and questions submitted to the Commissioner relating to the collection/use of fingerprints of employees for the purpose of checking their attendance at work, the Commissioner issued guidance relating to the collection of fingerprints for this purpose (which was posted on our website) and stressed that their collection for the above-stated purpose is *prima facie* contrary to the law and that it should only be used only in very exceptional/specific cases.

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 the Act No 101/2000 Coll., on the protection of personal data and amendments to some related acts, which entered into effect on June 1, 2000. The Office for Personal Data Protection (OPDP) was established on the basis of the provisions of this act and is endowed with strong powers, including taking measures and direct imposition of fines in case of breach of law, as well as with independent status. The act essentially implemented the 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.

The Directive 2002/58/EC was partly transposed in 2004 by the Act No 480/2004 Coll., on certain information society services, where particular provisions on unsolicited communications were embodied with a new strong competence for OPDP in combating "commercial spam". This directive was essentially subsequently implemented in 2005 by the Act No 127/2005 Coll. on electronic communications which simultaneously implements a number of other directives belonging to the "telecommunications package".

In 2007, there were the following two new developments in the basic data protection legislation:

- slight amendment of the Data Protection Act No 101 for the purposes related to the entry of the Czech Republic to the Schengen area (Act No 101 was amended by Act No 170/2007 Coll.), and
- opening of an amendment procedure of the Electronic Communications Act No 127 as a result of the need to transpose the Data Retention Directive No 2006/24/EC into national law; the procedure has not yet been completed.

B. Major case law

In accordance with the legislative rules of the Government of the Czech Republic, OPDP is the mandatory point to which the drafts of the relevant acts and other regulations for observation within the framework of inter-ministerial proceedings are submitted, therefore prior to submission of the draft to the Parliament. In 2007, OPDP expressed its opinions on a number of legal regulations.

The transposition of the Data Retention Directive will require, apart from the amendment of the Electronic Communications Act (see above), the introduction of changes into some other acts, mainly the Police Act No 283/1991 Coll. The Police Act is being amended anyway for other reasons. The draft was met by serious critical notes from OPDP and the procedure has not yet been completed.

Long-term preparations for the entry of the Czech Republic to the Schengen area culminated in 2007. On 1 September 2007, the Schengen Information System was put into service for testing purposes. At the end of September 2007, the evaluation mission of experts was closed with favourable conclusions. As a part of preparation activities several acts had to be amended, mainly:

- Act No 283/1991 Coll. (as amended), on the Police of the Czech Republic,
- Act No 41/1961 Coll. (as amended), on Criminal Court Proceedings (Criminal Order),
- Act No 326/1999 Coll. (as amended), on Residence of Aliens in the Territory of the C.R.,
- Act No 325/1999 Coll. (as amended), on Asylum,
- Act No 361/2000 Coll. (as amended), on Traffic on the Road Network,
- Act No 56/2001 Coll. (as amended), on the Conditions for the Operation of Vehicles on the Road network.

The position of OPDP as an independent supervisory body for the Schengen Information System was definitely confirmed. Finally, the Council Decision 2007/801/EC of 6 December 2007 confirmed the full application of the provisions of the Schengen acquis in nine countries including the Czech Republic.

C. Major specific issues

Control activities of OPDP in 2007 included a total of 112 completed inspections. Most of the inspections performed by independent inspectors and their control team were *ad hoc* actions based on instigations and

complaints of individuals. Only about 15% of inspections are based on the Plan of Control Activities, but this type of control action typically has a much more complex nature covering a wider scope of data processing features and aspects.

The Plan of Control Activities 2007 was focused on 5 main general topics:

1. Information systems of public administration, with special impact on data processing related to information on property of natural persons (e.g. the Cadastre of Real Estate);
2. Personal data processing under systems of surveillance (camera systems), with special impact on systems in education, healthcare and municipalities;
3. Readiness of the Czech Republic for the entry to the Schengen Area, mainly as a follow-up of the conclusions of the 2006 evaluation mission of experts;
4. Transport systems – special attention was paid to monitoring of movements of cars in road transport, e.g. in relation to toll collection;
5. Personal data processing in administration of justice and public prosecutor bodies.

The above mentioned control activities do not include those concerned with ***unsolicited commercial communications*** ("marketing spam"). 1569 complaints and other instigations concerning this particular area were received by OPDP in 2007; the related control actions were aimed at 515 entities of which 466 were ordered to take measures and financial sanctions were imposed on 71. As in the previous year, the most frequent problems can be summarised in the following points:

- 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.
- Almost no one declared the communication as a commercial communication. The messages have all sorts of designations – newsletter, info, news, etc. However, the Act on Certain Information Society Services stipulates that a commercial communication must be "clearly and plainly" designated as such.
- Some providers of internet services contribute to obfuscate the interpretation of the legislation in that they do not send out the commercial communications themselves, but insert advertising footnotes at the end of the messages they transmit, i.e. short advertising messages placed as a footnote to e-mail.
- For some providers of electronic services, demonstration of consent is limited to checking off a box in 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.
- If commercial communications are to completely comply 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 to send 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.

In addition to its standard supervisory activities, OPDP took great pains in communication activities: A specific *education program*, consisting of a four-hour course aimed at secondary school teachers focusing on privacy and personal data protection in the context of fundamental human rights, was developed by the Czech DPA and the Ministry of Education, Youth and Sport. Also an *amusing film* composed of 13 episodes on data protection issues was produced in cooperation with Czech TV and broadcasted on prime time for four months.

Last but not least, a *competition aimed at young people* "My Privacy! Don´t look, don´t poke about" was started on Data Protection Day and evaluated in April 2007. Young people in two age categories were encouraged to express in literal or graphic form what they understand by the notions of privacy protection and personal data protection. The awards were given to the winners at the International Film Festival for Children and Youth in the town of Zlín on 1 June 2007 on the 7th anniversary of the institution of the Czech DPA.

On 11 December 2007, the Data Protection Agency of the Community of Madrid awarded to OPDP the European Prize to Data Protection Best Practices in European Public Services.

Denmark

A. Implementation of Directive 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 at the following address: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/

The act implements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. Directive 2002/58/EC has been 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 780 of 28 June 2007),
- Executive Order No 1031 of 13 October 2006 on the Provision of Electronic Communications Network and Services,
- Chap. 71 of Law on Administration of Justice, cf. Exec. Order No 1261 of 23 October 2007
- Section 263 of the Penal Code, cf. Exec. Order No 1260 of 23 October 2007

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.

In 2007, the Ministry of Justice proposed legislation regarding security at certain sporting events (hooligan register).

According to the proposed legislation, the police could quarantine a person if he or she had been charged with a crime committed in connection with a specific sporting event, and if there was reason to believe that he or she, if not quarantined, would commit new crimes within the geographic area covered by the quarantine.

A quarantined person would be prohibited from attending certain sport events, and would be prohibited from going within 500 metres of those sporting events for a period of 6 hours prior to and 6 hours after the event. According to the proposed legislation, quarantine should be for a certain period of time of no more than 2 years.

According to the proposed legislation, the police should transfer personal data about quarantined persons to sports clubs in order for them to enforce the quarantine. Among the personal data transferred to the sports clubs would be names and photographs.

The DPA found that the proposed legislation caused doubts as to the protection of the privacy of the data subjects. The DPA doubted that the proposed processing of sensitive data would be adequate as regards to the purposes described in the proposed legislation.

The DPA emphasised that the proposed legislation would make it possible to process sensitive data about the data subjects even though they were only charged with a crime.

The DPA also emphasised that the proposed legislation could lead to the spreading of sensitive data to a broader circle of persons which again could lead to an increase in the risk of data being processed in breach of the Act on Processing of Personal Data.

In the latest draft of the proposed legislation many of the doubts pointed out by the DPA have been addressed by the legislator. However, the proposed legislation has yet to be adopted.

B. Major case law

The DPA was asked to give an opinion regarding the request of ATP[7] (*Arbejdsmarkedets Tillægspension*) to transfer personal data to third countries, cf. Section 27(4) of the Act on Processing of Personal Data.

The DPA was informed that, by the end of 2006, ATP had almost 4.5 million members and approximately 150,000 contributing employers, from both private and public sectors.

The personal data processed by ATP included information covering name, address, other contact information, civil registration number, employer, occupation and education.

ATP wished to transfer data about members and contributing employers to data processors in India and South Africa primarily due to security of supplies.

The DPA informed ATP about Section 41(4) of the Act on the Processing of Personal Data which states that: "As regards data which are processed for the public administration and which are of special interest to foreign powers, measures shall be taken to ensure that they can be disposed of or destroyed in the event of war or similar conditions".

After having corresponded with ATP the DPA concluded that Section 41(4) prevented ATP from transferring personal data to India and South Africa.

The DPA emphasised the nature of the personal data processed and the amount of data processed by ATP (covering almost the entire population of Denmark).

The DPA also emphasised that both personal data from the centralised civil register and personal data about citizen's education were mentioned, as information covered by Section 41(4), by the legislative power when the Act on the Processing of Personal Data was adopted.

C. Major specific issues

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

Inter alia, the decision was based on a recent opinion by the DPA, pointing out a series of questionable factors relating to the joint enforcement of the Act on TV surveillance and the Act on Processing of Personal Data.

Based on the opinion of the expert group, to which the DPA gave an opinion, new legislation was adopted by the Danish Parliament on 1 June 2007.

The main elements of the act are the following:

- Access for financial institutions, casinos, hotels, restaurants, shopping centres and retail shops to initiate TV surveillance of their own entrances and fronts of buildings. Surveillance of areas situated directly next to entrances and fronts, which naturally are or may be used as access or escape routes to and/or from their own entrances may only be initiated by financial institutions, casinos, hotels, restaurants, shopping centres and retail shops if it is clearly necessary for crime prevention purposes.
- Amendment of the Data Protection Act so that it covers any processing of personal data in connection with TV surveillance and contains specific rules regarding retention of data (30 days unless necessary for a specific case) and disclosure of data (disclosure may only take place with the explicit consent of the data subject, if the disclosure is specified by law or if the data is disclosed to the police for investigatory purposes).
- Notification to the DPA of processing in connection with TV surveillance is not required.
- The DPA is responsible for inspecting the processing of data in connection with TV surveillance by private controllers.

[7] Independent institution, established by Act No 46 of 7 March 1964, for the purpose of paying supplementary pensions to wage earners etc.

In its opinion, which was given prior to the adoption of the new legislation by the Danish Parliament, the DPA expressed support for the suggestion that only certain groups of businesses would be allowed to initiate TV surveillance in limited areas, and that the surveillance must be clearly necessary for crime prevention purposes.

The DPA underlined that the proposed legislation would lead to an increased processing of personal data, also concerning the people passing through the areas under surveillance.

In connection with the expanded access to initiate TV surveillance, the DPA stressed the necessity for adequate safeguards such as the adoption of rules regarding data retention and disclosure of data as well.

With regard to sound recording in connection with TV surveillance, the DPA requested that this matter be considered in connection with the adoption of the new legislation, because the current legislation, as opposed to the Data Protection Act, does not cover processing of personal data in connection with sound recording.

The DPA was favourable towards the suggestion that the DPA should not be notified about TV surveillance, partly due to considerations concerning the matter of resources, but also due to the fact that the DPA would be responsible for inspecting all data controllers who process personal data in connection with TV surveillance whether they are public or private.

Estonia

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

During the last accounting period, the development in the area was the completion of the draft legislations of Personal Data Protection Act (hereinafter PDPA), and Public Information Act (hereinafter PIA), passing the amendments of these acts and their partial entering into force may be considered as the most important development of the current period. Final implementation of two important pieces of legislation will be part of the next accounting period.

Changes in the way personal data are categorised, and the inclusion of biometric data in the category of sensitive data are the most significant features of the PDPA, which was passed on 15 February 2007 and which will fully enter into force in 2008. Also the increase of protection of personal data processing, i.e. changes in regulations about processing of personal data that is provided for legal public use, regulations of processing personal data for research or government statistics and establishing an institution of an official responsible for personal data protection.

Since 1 January 2008, the category of private personal data no longer exists. Personal data is divided into sensitive personal data and personal data. With the vitiation of the private personal data category, the aforementioned duty of notification of processing data will also be invalidated.

Since 1 January 2008, biometric data, principally fingerprint images, palm prints and iris images, is being treated as sensitive personal data and data relating to genetic information has been replaced by the term "genetic data".

One change the law prescribes is that a person has a right to demand the termination of disclosure and any other usage of personal data, which has been lawfully designated for public use. Therefore, a person will retain control over further usage of this data after its disclosure, which the previous wording did not allow.

Since 1 January 2008, the PDPA regulates collection of personal data for solvency assessment. While according to the norms valid up to this point, the time limit for collection of such data was not specifically provided, then from 1 January 2008, the data about personal payment default may only be processed and communicated to third persons within three years from the violation of obligations. Hence, the data in the cedit register cannot be older than three years. Older data shall be removed. Essentially, the goal of this amendment is to ensure that each processor ensures the basis for processing the data and ensures that contracts, agreements and other documents are not contrary to the requirements of the law. The requirements concerning the consent of the data subject changed as well.

In future, a person can prohibit the processing of data where the legal basis for its disclosure and processing cannot be verified.

The only cases in which a person cannot prohibit further processing are if the original disclosure took place for journalistic purposes (there are new relevant provisions in the law) or on the basis of law (for example, databases accessible only to government authorities).

B. Major case law

Case 1: Disclosure of personal data on the website of Tallinn City Government
A private individual turned to the DPA with an explanation application and asked for an explanation for the following: on what legal basis has his child's name been disclosed in Tallinn City Government's legal acts registry to which public access has been granted. The person said personal data had been disclosed to which the access of third persons should be restricted.

DPA approached Tallinn City Government about this matter and explained its position to Tallinn City Government officials. DPA gave its written position on disclosure of personal data in legal acts of Tallinn City Government and, based on the complaint of a private individual, asked for the removal of the name of the individual's child from the legal acts registry, published on Tallinn City Government's website. In response to this position, Tallinn City Government did not remove the child's name from the registry by the specified date.

Pursuant to the Local Government Organisation Act, rural municipality or city legislation may be disclosed and made accessible to everyone, pursuant to the procedure provided by law and the statutes of the rural municipality or the city. But pursuant to the same law, the data, the issue of which is prohibited by law, must not be disclosed.

Pursuant to §1 of the PDPA, the purpose of this act is to protect fundamental rights and freedoms of natural persons in the course of the processing of personal data in accordance with public interests. In the processing of personal data, chief processors and authorised processors of personal data are required to take guidance from the principles of purposefulness and minimality (§6(3) of PDPA) and from inviolability of private life.

The Data Protection Inspectorate argues that while a person's name itself does not qualify as private personal data, with additional information a person's name can also be private personal data. From the position of fundamental rights protection, it is extremely important that personal data is processed no more than needed for particular previously determined purposes.

Pursuant to the PIA, if the grant of access to information may cause the disclosure of restricted information, it shall be ensured that only the part of the information or document to which restrictions on access do not apply may be accessed (§ 38(2) of the PIA).

We explained to the City Government: according to the example of Article 1(1) and recital 10 of the preamble of the European Data Protection Directive 95/46/EC, the draft legislation of PDPA stresses, on specifying the purpose, the need to protect people's fundamental rights and freedoms, mainly the right of inviolability of private life. But this does not indicate absolutisation of the right for personal data protection and inviolability of private life, it just stresses that on completing personal data processing, in borderline cases, we should always give preference to the interpretation which protects inviolability of private life over possible public interests.

The conflict between protection of private life and the need for disclosure of data emerges clearly when data is disclosed on the Internet. The combined effect of the PIA and the PDPA is to prohibit the disclosure of private personal data and sensitive personal data (except in cases prescribed by law). Non-sensitive data can be disclosed only after balancing the competing interests involved: if disclosure would breach the inviolability of private life of the data subject, non-sensitive data cannot be made accessible to the public. Here it is important to note that limits are valid only for disclosure to the general public.

Based on the aforementioned, the Data Protection Inspectorate found that Tallinn City Government had violated the principles of minimality and purposefulness, where disclosure of data on the Internet is not proportional with the specified purpose and infringes on the inviolability of private life.

The Data Protection Inspectorate issued a precept to Tallinn City Government, where Tallinn City Government was obligated to remove the name of the private individual's child from the legal acts registry, published on the website of Tallinn City Government, by 15 January 2007.

Case 2: Credit register

There was an "Ego" hire-purchase contract entered into by private individual H.R. and Hansapank, and accordingly, H.R. was able to use credit, he also made a commitment to pay this credit back to Hansapank by monthly payments in accordance with the terms of the contract. H.R. failed to perform his contractual repayment obligation.

After that, Hansapank and H.R. entered into a debt contract for repayment of the debt, arising from the "Ego" hire-purchase contract. H.R. repeatedly failed to repay the amount of debt he took under the aforementioned contract.

Based on Section 88(2) (4) of the Credit Institutions Act and "Ego" hire-purchase contract and debt contract, Hansapank disclosed H.R.'s debts on the website of AS Krediidiinfo.

H.R. paid his debt to Hansapank in 2006 and requested the removal of his data from the Credit Registry.

Subsequently, H.R. made a complaint to the Data Protection Inspectorate. The Data Protection Inspectorate issued a precept to Hansapank: according to the complaint of the data subject, he did not give permission for his personal data to be disclosed on the website of AS Krediidiinfo. Since Hansapank did not specify the purposes of data processing in the contract nor, to the knowledge of the Data Protection Inspectorate, in any other documents related to the data subject, then based on the principle that in the case of a dispute, a data subject is presumed not to have granted consent for the processing of personal data relating to him (Section 12(5) of PDPA), disclosure of data by Hansapank without the consent of the data subject being considered as data processing.

The notice obliged the bank to cease illegal disclosure of H.R.'s personal data. Hansapank complied with the notice, but sent its objection to the notice to the Data Protection Inspectorate. The Data Protection Inspectorate did not agree with the objection, so Hansapank sought recourse in the Court.

The Tallinn Administrative Court found in its decision of 17.4.2007 that, in its final conclusion, the precept was substantively justified and legitimate.

On 14 May 2007, Hansapank filed an appeal to Tallinn Court of Appeal.

C. Major specific issues

For the first time in this period, the Data Protection Inspectorate formulated its own initiative concerning supervisory operations priorities for the year. There were seven topics chosen that were dealt with in-depth on this occasion and for each of them the inspectorate published an opinion or an instructive document on its website, through the media or a channel available to the interest groups. This was an initiative from within the organisation and we chose the topics which the officials of the inspectorate found to be the most problematic or hard to interpret in the areas of personal data protection and public information.

On the basis of the topics, we conducted an analysis and supervision, if required, and in accordance with the results prepared guidelines/guidance documents which have been published on the Data Protection Inspectorate website.

The operations priorities chosen in the stated period were the following: transmission of personal data to third countries; dangers or possibilities in the world of web-search; admissibility of recording phone calls; disclosure of personal data in legal instruments of local governments; processing of personal data within the ID-ticket project; child and his or her rights in personal data processing, and, finally, the composition of personal data in issuing customer cards.

We will give a brief overview of two opinion documents of interest:

Processing of personal data within the ID-ticket project

According to the Identity Documents Act, the primary and only compulsory identity card in Estonia is the ID card. The document "Processing of personal data within the ID-ticket project", published by the Data Protection Inspectorate, studies the usage of the ID card as proof of purchase of service using the example of Tallinn's ID-ticket system, mainly focussing on data processing in such systems.

The guideline is mainly intended for public and private organisations who wish to create information systems that use the ID card as proof of right to receive a service or a product. The Data Protection Inspectorate formulated seven suggestions on the basis of personal data protection principles.

The Data Protection Inspectorate established that the system, based on the ID card for purchasing the right to use public transport, which is used in Tallinn, is in conformity with the principles of the PDPA. The Data Protection Inspectorate welcomes initiatives that allow the broadening of the field of ID card application and at the same time take account of citizens' right of relevant personal data protection from all perspectives.

Children and their rights in the processing of personal data

The Data Protection Inspectorate analysed the processing of children's personal data in various everyday areas.

The published information is based on main international legal instruments about children's rights, on domestic norms of relevant areas, on the results of conducted monitoring and on behavioural patterns in different environments that are used in practice. In accordance with the Child Protection Act, persons under the age of 18 are considered children. The document presents a legal argumentation about processing the personal data of a child and a child's right for inviolability of private life.

A separate paragraph analyses questions connected to web-cameras at schools. Technology allows parents to monitor their children 24 hours a day and the need for video monitoring is based on security considerations. At the same time, recording any kind of data on videotape affects the fundamental rights of a person.

The Inspectorate has made a recommendation in the document that on the one hand, monitoring children's actions must be proportional to child's right for privacy and, on the other hand, be based on public interests like security and prevention of criminal offences, etc.

In addition, the published document analyses the areas that concern disclosing children's marks, disclosing children's data on the Internet and more attention has been paid to the topic of exposing children in the media.

In brief, we have taken the position that protection of the privacy of children should be based on two aspects: responsibility and awareness.

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

B. Major case law

The Court of Justice of the European Communities processes the publication of data on earned income

A Finnish company annually published the earned income of over one million Finns and passed the data on to another company for the purposes of an SMS service. This information was then passed on to the public for a fee as a commercial SMS service.

The Data Protection Ombudsman asked the competent Data Protection Board to forbid the publication of this information on earned income. The Data Protection Board has the jurisdiction to prohibit illegal processing of personal data. Contrary to the view of the Data Protection Ombudsman, the Data Protection Board, and the administrative court processing the matter after the Board, accepted the interpretation that this was a case of processing personal data for a journalistic purpose, to which the Personal Data Act is not principally applied. The processing of the matter is ongoing at the Supreme Administrative Court. On 8 February 2007, the Supreme Administrative Court requested a preliminary ruling from the Court of Justice of the European Communities, which has arranged a hearing on the matter on 12 February 2008. The Supreme Administrative Court will base its decision on the preliminary ruling.

The Supreme Administrative Court orders a bank to implement the right of full access

In February 2007, the Supreme Administrative Court agreed with the interpretation of Finnish law by the Data Protection Ombudsman in which the right of access extends to data on a client's own loan transactions and the interest rates used for them.

The bank had argued that transaction statements and interest rate data are not part of the client data files, since the microfilms containing this data are stored separately from the client data file. However, according to the Data Protection Ombudsman, this view is erroneous, because the extent of the personal data file is determined by its use. According to the Personal Data Act, data processed in order to attend to the same task belong to the same personal data

file (logical data file), even though various parts of the data file (sub-registers) are stored separately. Because the purpose of using the interest data was, like other data on X, the management of a client relationship, all the data was part of the same data file. Whether it was technically stored together or apart was deemed irrelevant.

Authentication of the client in quick loan companies

The demand for quick loans requested via mobile phone or over the Internet has dramatically increased in Finland. It is estimated that there are currently 50 to 60 quick loan companies. Inadequate authentication of quick loan applicants has led to a number of cases where the loan has been taken in another person's name without them being aware of it.

In many of the quick loan companies, authentication of the loan applicant is based solely on the social security number given by the applicant and subscription data from the telecommunications company. If this data checks out, it is assumed that the applicant is who he/she claims to be. Inadequate authentication has led to identity theft. Authentication difficulties are complicated by the fact that a specific obligation to identify the quick loan applicant has not been imposed on the creditor.

In March 2007, the Data Protection Ombudsman asked the competent Data Protection Board to order a quick loan company to change their authentication process pertaining to loan applicants. The Data Protection Ombudsman required that creditors identify their clients in order to ensure the accuracy of any personal data processed. The view of the Data Protection Board will have even more general significance, since according to a survey commissioned by the Data Protection Ombudsman, almost all businesses in the field use a similar system based on weak identification. The decision may have repercussions on other fields of business as well.

C. Specific issues

Credit Information Act

The new Credit Information Act entered into force on 1 November 2007. The Act brings together provisions on credit information about consumers, companies, and relevant company personnel. The Act includes provisions on data to be stored in credit reference records, and the period for storage of the said data. The new Act defines more closely the purposes for which credit information on consumers may be disclosed and used.
Under the new Act, the Data Protection Ombudsman also oversees the processing of credit information on companies. The providers of credit information are expected to be trustworthy and to follow good credit information practice. Currently, information on the disruption of payment confirmed by authorities and notified by the debtors, as well as the credit ratings of individuals and companies can be stored in the credit reference records.

Information on any default on payment is stored in the credit reference records for a predetermined period of time. These storage times are made more precise, and in some cases shortened in the new Act. While payment of debt may shorten the storage period on the one hand, the storage period can be extended, on the other, if the individual or company in the register is again guilty of default on payment.

The new Act will also allow companies to check their credit information and to correct any errors. Previously, such rights were only granted to natural persons. The providers of credit information must also give credit information to consumers for reasonable compensation. The aim is that consumers can better ascertain the reliability of their contracting party.

Act on electronic processing of social welfare and health care patient data

The act on electronic processing of social welfare and health care patient data entered into force on 1 July 2007. A nationwide electronic patient database is being created in Finland, with the whole of the health care sector as users. The database is being implemented by the Social Insurance Institution of Finland, and will be gradually brought into operation from 2008 until 2011.

The database comprises storage, archiving, and transfer services of patient documents and prescriptions. The reform aims to improve the co-operation between various parties in the field of social welfare and healthcare

and to enable the electronic transfer of data from one unit to another if the patient gives his/her consent.

The main goal is to promote security in the processing of social welfare and healthcare patient data and the production of healthcare services in a manner that is both safe for patients and effective. In addition, the new act also allows patients access to their own data and log data pertaining to its use by, for example, viewing them online.

All public healthcare providers are required to start using the data system services. Private healthcare providers are obliged to join the system if the long-term retention of their patient data is conducted electronically.

Electronic Prescriptions Act

The new Electronic Prescriptions Act entered into force on 1 April 2007. The new legislation determines the requirements set for an electronic prescription system and its implementation. According to the Act, prescriptions can be drawn up electronically and transferred via data networks to the national prescription centre, which provides the information needed by the pharmacist to provide the prescription.

Physicians must tell their patients about the use of electronic prescriptions and give them written instructions on the medicine and its use. The patient has the right to refuse the electronic prescription, in which case he/she will be provided with a traditional written prescription. Because all the electronic prescriptions are stored in the prescription centre, the patients can, at any time, check the validity of their prescriptions and the amount of undelivered medicine without them having to hold on to the original prescriptions. The prescription centre and prescription archives will be maintained by the Social Insurance Institution of Finland. Prescriptions will be kept in the prescription centre for 30 months, after which they are to be transferred to the prescription archive.

If all the prescriptions of a patient have been drawn up electronically, a physician, dentist, pharmacist or qualified chemist can check the overall medication received by the patient and potential drug interactions on the basis of data provided in the prescription centre (and with the patient's consent). Patients also have the right to receive information on who has processed or looked at data pertaining to them in the prescription centre or prescription archive.

Recommendations of the working group on biobanks

According to the report of a working group appointed by the Ministry of Social Affairs and Health issued on 12 October 2007, the wider use of both existing and future collections of human tissue samples for medical purposes requires supervision of the activities, increased communications, more uniform procedures, and quality criteria.

The working group proposed that biobanks be founded in Finland (decentralised system). The key task of a biobank would be to collect, manage, and store human-based biological samples and information derived from them or pertaining to them for future research. A biobank can either collect the samples themselves, or research sample collections from elsewhere can be incorporated into the biobank.

According to the working group's proposal, a sample donor would be asked for permission to transfer their sample to the biobank. Consent would be based on the knowledge of the general purpose of the biobank. Sample donors have the right to know about the use of their samples and the opportunity to influence their use is guaranteed by the general reporting obligation, transparency of the activities, and supervision by authorities pertaining to biobank operations. The transferral of already existing diagnostic and research samples taken for diagnostics and treatment of diseases to a biobank is possible either with the consent of the sample donor or, if renewing consent is unreasonably difficult, through permission of the National Authority for Medicolegal Affairs.

Data on biobanks is collected in a biobank register which, together with the biobank-specific sample collection registers, forms a data system serving the information access needs of researchers and the general public alike.

France

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

1. Decree of 25 March 2007

France transposed the European Directive of 24 October 1995 into national law with the act of 6 August 2004, amending the act of 6 January 1978. The first implementation decree of this new act was adopted on 20 October 2005 and contained, in particular, provisions on the designation of data protection officers within companies and administrations. An amendment to this decree, adopted on 25 March 2007, introduced particular procedural specifications.

- Notification of persons in the event of transfer of their data outside the European Union.

The decree of 25 March 2007 states that persons whose data is transferred outside the European Union must not only be informed of this transfer, but more precisely informed of the country of the recipient institution, the purpose of the transfer, the categories of personal data involved in the transfer and the level of protection provided by the third country located outside the European Union. Furthermore, the decree provides that where the transfer occurs after the collection of the personal data, it may only take place within a period of fifteen days following the receipt of the above mentioned information by the data subject.

- Right of access procedure

The implementation decree of 25 March 2007 sets out the provisions for exercising the right of access. The request for right of access can be made by mail or on site. The person making the request must provide proof of identity to the data controller in any form required. Where the request is made on site and cannot be met immediately, a dated and signed acknowledgement must be sent to the person making the request. In accordance with the decree, the data controller must respond to the request from the data subject within two months of its receipt. After a period of two months, the failure of the data controller to respond is considered a refusal.

2. Opinion on the draft decree concerning the application of Article 6 of the Act of 21 June 2004 on Confidence in the Digital Economy transposing Directive 2000/31/CE into French law

Article 6 of the Act on Confidence in the Digital Economy (LCEN) imposes an obligation to keep identification data of persons who have contributed to the creation of online content.

This article obliges hosting and Internet service providers to keep identification data of persons who have contributed to the creation of online content (blogs, personal sites, advertisements on Internet auction sites) in order to communicate it, if necessary, to the judicial authorities and the services responsible for the fight against terrorism.

The National Commission for Information Technology and Civil Liberties (CNIL) recently examined a draft decree defining the categories of data concerned and the period for which they are to be retained. This decree and the opinion of the CNIL will be published soon.

B. Major case law

1. Diversity

After publishing its first recommendations on the subject in July 2005, the CNIL extended its considerations by holding more than sixty hearings with researchers, statisticians, trade union organisations, representatives of major religions, collective organisations, experts and company directors. A wide range of viewpoints, some of them diverging, were expressed during these hearings, highlighting the difficulty of reaching a consensus in this field.

The CNIL was nevertheless able to make an observation. France must improve its statistical machinery and there are measures that can already be taken to improve the extent of knowledge about our society and, at the same time, to better combat discrimination.

In this respect, the CNIL published ten recommendations in May 2007, which were commended for their pragmatism, balance and ambition. The main points of these recommendations are the following:

- It is vital to allow persons seeking information easier access to personnel files, administrative files and public statistical databases in adherence, of course, to data protection provisions.

- To establish if discrimination has been experienced, surveys using questionnaires should be conducted with the persons concerned. As they are optional and based on self-declaration and the answers are confidential, questions may be asked on the person's nationality and place of birth, and also about their parents. It is also important that the persons who feel discriminated against indicate the criteria - physical appearance, language, name - on which they think this discrimination is based.
- Furthermore, the analysis of Christian names and surnames may in some circumstances, - i.e. when it does not result in classification into ethno-racial categories - be useful for identifying possible discriminatory practices.
- In this respect, the CNIL has major reservations about the creation of an ethno-racial reference system. The vast majority of the persons consulted were opposed to this kind of classification system. The risk of reinforcing stereotypes, stigmatisation, ambiguous, unscientific, narrow or approximate classification are among the many reasons that explain current reticence and endorse a very careful approach to this subject. The CNIL found, in particular, that the decision in principle to create such a classification system, if its use is to be mandatory, in particular for government statistics and census taking, should rest with the legislator under the control of the Constitutional Council.
- Finally, data protection legislation must be amended to ensure better protection of people and their sensitive data, guaranteeing the scientific nature of research and strengthening the control of the CNIL over research files where the consent of persons alone is not sufficient.

Following up the recommendations of the CNIL, Michèle Tabarot and Sébastien Huyghe, both representatives and members of the CNIL, presented an amendment to the draft act on immigration control, integration and asylum, aiming to make the processing of data, directly or indirectly revealing the racial or ethnic origins of persons for the requirements of studies aiming to establish "*the degree of diversity of the origins of people, discrimination and integration*", subject to the authorisation of the CNIL. In order to ensure the scientific quality of these studies, it was foreseen that the CNIL would have recourse to a committee appointed by decree. In order to avoid creating a new structure, it was foreseen that the authority would have recourse to the Scientific Council of the Conciliation Committee for data in the fields of human and social sciences created by the ministers of the economy, employment, national education and research.

This provision was the subject of an appeal to the Constitutional Council.

In a decision of 15 November 2007, the Council declared it contrary to the constitution, finding that this provision bore no relationship to an act on the entry and residence of foreigners in France. In essence, the Council declared that: "*while data processing required to carry out studies on the extent of diversity of the origins of persons, discrimination and integration may use objective data, they may not be based on ethnic origin or race without failing to adhere to the principle set out by Article 1 of the Constitution.*"

This decision leaves open the question of knowing which types of study can today be conducted in the field of establishing diversity, discrimination and integration. Recent statements from the Constitutional Council on the judgement that it made on 15 November 2007 provide further clarification and suggest the use of an ethno-racial reference system is prohibited, while studies on the effects of ethnicity are permitted.

2. Tracking Internet users

In October 2005, the CNIL refused the implementation of four peer-to-peer network surveillance systems requested by collecting companies specialising in the assignment of rights in the music industry (SACEM, SDRM, SPPF and SCPP). These four companies disputed the decisions of the CNIL before the Council of State, which partially annulled them on 23 May 2007. It effectively found that the CNIL had committed an assessment error, deeming the data processing to have been for the purposes of research and establishing illegal provision of musical works on the networks to have been disproportionate. However, the Council of State accepted the analysis of the CNIL on the procedure for sending educational messages targeted at Internet users. It found these dispatches to be illegal, as they do not constitute cases where Internet access providers are authorised to retain the connection data of Internet users.

Following this decision, the CNIL approached the relevant collecting companies specialising in rights assignment, in order to establish their intentions. Three of them (SACEM, SDRM, SCPP) renewed their requests after removing the invalidated educational elements. In November 2007, drawing on the conclusions of the decision of the Council of State, the CNIL authorised these three companies to implement the system for processing research and establishing offences on the Internet. The final company concerned (SPPF) renewed its request in December 2007. The implementation of this system, identical to the other three, should receive authorisation at the beginning of 2008.

At the same time, in two judgements of April and May 2007, the Court of Appeal in Paris found that the IP addresses collected during research into and establishment of counterfeiting on the Internet do not allow the identification, even indirectly, of natural persons and that they do not constitute personal data. The CNIL, concerned about the effects of such analysis on the protection of privacy on the Internet, approached the Chancellery and the public prosecutor at the Court of Cassation in order to bring an appeal against these two judgements in the interests of the law. The CNIL pointed out that the data protection authorities of the Member States of the European Union stated, in an opinion of 20 June 2007, that the IP address does constitute personal data.

The CNIL also carried out several verification checks at the premises of companies providing peer-to-peer network surveillance services. The analysis of the findings made during these checks should be completed in the first quarter of 2008.

At this point, it should also be underlined that, in July 2007, the Minister of Culture and Communication established a board responsible for finding solutions to "*combat illegal downloading and to foster the legal provision of works*." This board, led by Mr. Denis OLIVENNES, presented several recommendations in November 2007. Their taking into account by the government should involve legislative and technical arrangements, on which the CNIL should express an opinion.

C. Functioning and activities of the CNIL

1. Adoption of rulings

In 2007, the CNIL was in session 40 times during 25 plenary meetings, 12 restricted committees and 3 deliberative committees. These meetings led to the adoption of 393 rulings (30% more than in 2006, and 600% more than in 2003).

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

a. Advice and expertise

In 2007, the CNIL expressed 6 opinions on draft acts and decrees, including its opinion on the draft decree on the application of Article 6 of the Act of 21 June 2004 on Confidence in the Digital Economy, and on the retention of data allowing the identification of any natural or legal person having contributed to the creation of online content.

b. Simplifying prior checking formalities

Continuing the work undertaken in this regard, the CNIL adopted measures simplifying prior checking formalities in execution of its services. It therefore adopted four single authorisations (including one authorisation concerning the implementation of the automatic processing of personal data with regard to the management of offences by the public transport police and a modification of the authorisation concerning the processing of personal data carried out in financial organisations as part of the fight against money laundering and the financing of terrorism) and expressed two opinions on a single regulatory ruling.

These simplifications are systematically accompanied by very precise frameworks. They are not applicable if those responsible for the processing do not adhere to all of the related conditions set by the CNIL.

c. Reporting formalities

In 2007, the CNIL adopted:

- 214 authorisations;
- 26 refusals of authorisation;
- 22 opinions on data processing that is sensitive or harmful.

d. 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.

During 2007, the CNIL levied the following totals:
- 9 fines from €5,000 to €50,000;
- 5 warnings;
- 101 formal notifications.

2. Referrals
In 2007, the CNIL received 7115 referrals (4,455 complaints and 2,660 requests for the right to indirect access to police/gendarmerie files). The sectors most affected are: *banking*, *commercial prospecting*, *employment and telecommunications*.

This figure increased by 20% compared to 2006. The CNIL today receives twice as many complaints as ten years ago.

3. Major issues in 2007
Establishing a framework for biometrics
In 2007, the CNIL examined a voice recognition system for the first time. This is a system that aims to secure and facilitate the management and resetting of passwords used to access the IT system of the company Michelin. This method enables passwords to be generated and reset automatically. In particular, the CNIL checked that employees were well informed and that all measures had been taken to ensure data security and to prevent risks of identity theft.

The CNIL also examined for the first time five systems, based on the recognition of the venous plexus of the right hand, designed to control access to premises or IT systems. After carrying out in-depth technical analysis of this technology, the CNIL found that the venous plexus, at the current stage of technological development, is a biometric system without traces, and that its recording in a database does not involve specific risks with regard to data protection.

In 1997, the CNIL expressed for the first time its opinion on a system based on the recognition of fingerprints. Ten years later, it considered it necessary to redefine its position. It wished to set out the main criteria it applies to authorise or refuse the use of fingerprint recognition systems with storage on a reader-comparison terminal or on a server.

This analysis framework is based on the following observations:
- The fingerprint system is a biometric system with traces. Everyone leaves fingerprint traces, which are reasonably easy to use, in many situations in modern life. For example, on a glass or a door handle etc.;
- These "traces" can be captured without the person's knowledge and used, in particular, to steal their identity (usage of the fingerprint sample captured to defraud a fingerprint recognition system).

Taking into account these specific characteristics and associated risks led the CNIL to differentiate between systems according to the method of storing fingerprints:
- Storage on an individual data support (such as a smart card or USB memory stick): the risk is limited because the person has control of his biometric data, which cannot be used to identify him without his knowledge.
- Storage on a reader-comparison terminal or on a server: the risk is increased because the person loses control of his data, which is held by a third party. In the event of intrusion into the system, all prints can be accessed.

Therefore the Commission only authorises the implementation of fingerprint recognition systems with recording in a database if they are justified by a major security requirement and meet four conditions:
- The aim of the system must be restricted to controlling access of a limited number of persons to a well defined area, representing or constituting a significant requirement extending beyond the narrow interests of the organisation, such as the protection against physical harm of persons, goods, systems or certain information;
- Proportionality: it is important to establish whether the proposed system is well adapted, or as well adapted as possible, to the previously defined objective with regard to the risks that it involves in terms of the protection of personal data;
- Security: the system must allow both reliable authentication and/or identification of persons and provide

comprehensive security guarantees to prevent the data being divulged;
- The information on the persons concerned: it must be handled in adherence to data protection provisions and, where applicable, the code on labour law.

SWIFT affair – nearing an end to the crisis
In June 2006, the American press revealed the existence of an international banking transactions surveillance programme set up by the CIA shortly after the attacks of 11 September 2001. These revelations indicated that the CIA and the US Department of the Treasury had for years been taking advantage of access to millions of items of data transferred by SWIFT, which is the main international messaging network used in the banking sector (see 2006 Annual Report).

This access, established as part of the fight against the financing of terrorism, allows not only the surveillance of financial transfers to the United States, but also all other types of transaction handled by SWIFT, including within the European Union. The transaction amount, the currency, the value date, the name of the recipient, the client who requested the financial transaction and the client's financial institution were also communicated. The official objective of this programme is to identify persons suspected of being connected to the financing of terrorism. But concerns about usage for economic, rather than security, purposes cannot be ruled out.

In its opinion of November 2006, the Coordination Group of the European Data Protection Authorities (Article 29 Working Party or G29) found that SWIFT had not adhered to European data protection regulations, in particular by lending its support to the implementation of the banking and financial data surveillance programme of the American authorities. The Working Party also found that the financial institutions also bore partial responsibility in this matter.

A year on, and an end to the crisis is apparent. The G29 issued a press release on 11 October 2007 welcoming the significant progress made by SWIFT in bringing its activities into line with data protection principles.

The completion of negotiations between Europe and the USA
In spring 2007, The European Commission and Council negotiated a number of guarantees with the American government in order to define rules concerning the usage of data stored in the United States in the SWIFT database by the American authorities. These guarantees concern the limitation of usage to the fight against terrorism, adherence to the principle of necessity, retention periods of 5 years, the nomination of an "eminent European figure" with responsibility for verifying the correct functioning of the surveillance programme (Mr. Jean-Louis Bruguière). This political agreement was the subject of correspondence, which has been published by the European Commission.

A complete restructuring of the technical architecture
SWIFT's current architecture is based on the principle of systematic copying of all messages in two operational centres, one in the Netherlands and the other in the United States. These messages are therefore currently stored for 148 days in the American operational centre irrespective of their origin and destination.

However, this architecture will be completely overhauled at the end of 2009 with the setting up of a new operational centre in Switzerland. The messages sent by the clients of European banks will be systematically copied in the two European centres (Switzerland and the Netherlands), and will no longer transit through the American server. American surveillance will therefore no longer be carried out, in particular on messages concerning intra-European Union transfers. The messages originating from or destined for the United States will be systematically stored in the American operational centre.

Discovery
The CNIL has observed a recent increase in the requirement for the communication of personal data held, *inter alia*, by the French subsidiaries of American companies that are the subject of discovery proceedings before American civil courts or pre-trial discovery. The companies subject to these demands, or their subsidiaries abroad, frequently find themselves obliged to communicate copies of hard disks or electronic messages of certain employees or their entire staff.

Furthermore, under a different legal system, some foreign authorities, such as the *Securities and Exchange Commission* (SEC) or the *Federal Trade Commission* (FTC), can also demand that foreign companies produce documents using their powers of investigation. Such injunctions can concern French companies, when according to which, they are subsidiaries of American companies focusing on the American market, or are operating directly in the American market.

This raises various issues with regard to data protection legislation in particular.

These demands for communication of information may contravene data protection provisions, in particular with regard to notification and gaining the consent of the persons concerned, the proportionality of the processing carried out and provisions concerning the transfer of data outside the European Union.

Such cases also raise problems concerning other fields besides data protection law, in particular international judicial cooperation, the protection of national economic interests and national sovereignty.

Concerned about the consequences of these obligations and the communication of such quantities of data with regard to the applicable French and European regulations, a number of French companies and foreign companies set up in France, and lawyers specialised in this field, have alerted the CNIL to the development of this phenomenon.

Worryingly, these companies also express doubts about the protection of their industrial and commercial secrets, and some of them raised genuine concerns about economic intelligence.

In view of the increase in the number of companies concerned that are now contacting the CNIL, it has attempted to draw the government's attention to this issue. Interministerial discussions are set to take place soon.

Central files on credit and housing

The establishment of files providing an entire economic sector – credit institutions and loan providers – with information on solvency risks presented by applicants for loans or housing requires a high degree of caution from the CNIL, taking into account the risk of social exclusion of the persons concerned.
In particular, the issue of legitimacy and proportionality of the introduction of a credit database in France raises questions in terms of ethics and infringement of privacy, as well as in terms of efficiency and costs. The CNIL has always refused to recognise the legitimacy of the setting up of such a system in the absence of a specific legal framework. It considers that only the legislator has the authority to give a ruling on the social benefit of a "positive file" in the credit sector and to set out, if necessary, the objectives and content of this database. In line with this position, it refused to authorise the implementation of a credit database by the company Experian.

Furthermore, it refused the company, Infobail, authorisation to implement two data processing systems concerning information for property market professionals on the management of outstanding payments and the surveying of tenants of residential property with regard to their payment obligations, because these files are detrimental to the right to housing established by the legislator, which is responsible for ruling on the opening of a negative or positive file in the housing sector.

Checks on personal medical file (DMP) tests

The CNIL carried out around 18 on-site checks at the premises of the main parties involved in the DMP tests, including hosting providers, hospital centres, healthcare networks, self-employed doctors and call centres. As a result of these checks, it made the following observation.

The CNIL observed that some hosts electronically transferred the usernames of patients to healthcare institutions without special protection. Some call centres permit, in the event of the loss of usernames, consultation or feeding of the DMP, sending a password to patients by unencrypted e-mail, or communicating this password to them by telephone. These practices compromise the confidentiality of this information.

The CNIL also revealed that the patients were not always clearly informed that access to the medical data contained in their DMP files required an Internet connection.

Furthermore, they were sometimes informed that access to this data was possible through an intermediary at the host's call centre, whereas in fact the latter's responsibility was only to provide technical assistance for patients or to enable them to update the administrative data concerning them, their password or the composition of their circle of trust.

A shortfall was established in measures implemented at the call centres for identification and authentication, while the authentication of patients based on verification using challenging questions (for example, the name of your mother-in-law, the make of your first car) provided by patients during registration was not carried out systematically.

Hosts also proposed providing access to the DMP files from their Internet site, using a basic username and password, for care organisations that do not issue their healthcare staff with CPS cards (healthcare professional cards). This solution was not accepted and is clearly contrary to the CNIL decisions of 21 March and 30 May 2006.

However, it was verified that administrative and technical staff of the hosts and the call centres do not have access to the healthcare data contained in the DMP files.

Germany

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

Directive 2004/82/EC of 29 April 2004 (API Directive) was transposed into domestic law by the third act on the amendment of the Federal Police Act of 22/12/2007. It will enter into force on 1 April 2008.

According to this Directive, as a minimum requirement, a certain data set has to be transferred by air carriers. It is true that when transposing the Directive into national law, Germany went beyond this data set. However, in the course of the legislative procedure, the BfDI succeeded in convincing the legislator not to realise their original plans but to add only the "gender" and the "visa number" to the data set to be transferred by air carriers to German federal police authorities. Both the air carriers and the federal police have to delete the data within 24 hours after their collection and/or transfer.

The PNR Agreement concluded with the USA in June 2007 including the accompanying exchange of letters between the US Department for Homeland Security (DUS) and the EU was transposed into national law by the act of 20 December 2007 without any amendments. It entered into force on 30 December 2007.

On 31 December 2007, the act on the new regulation of the surveillance of telecommunications and of other covert investigative measures and on the implementation of Directive 2006/24/EC (Federal Law Gazette (BGBl.) I, No 70 of 31/12/2007, p. 3198 et seq.) entered into force. The act foresees the retention of telecommunications, e-mail and Internet traffic data for six months, whereas the mandatory retention of Internet traffic data will be applicable as of 1 January 2009 only. Through this all the telecommunications traffic of all citizens of the Federal Republic of Germany will be registered, although presumably only an extremely small part of this enormous data volume is intended to be recalled by law enforcement authorities. In view of the jurisdiction of the Federal Constitutional Court there are doubts about the constitutionality of this data retention for later use for purposes that cannot be sufficiently determined.

The Conference of the Federal and "Länder" Data Protection Commissioners has time and again emphatically spoken out against the legal introduction of the retention of telecommunications traffic data for later use and the tightening of covert investigative measures in connection with criminal proceedings, which the act foresees as well.

Numerous constitutional complaints have been lodged against that act with the Federal Constitutional Court.

With the act amending the act on passports and further regulations of 20 July 2007 (BGBl. I, No 35 of 27/7/2007, p. 1566 et seq.) with effect from 1 November 2007 in the Federal Republic of Germany, the second-generation electronic passport (e-passport) was introduced. Data of both forefingers, in addition to the photograph, are stored in the biometric chip of that passport. Thanks to this, the Federal Republic complies with the "Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States". The legislator excluded the establishment of a nationwide database (Art. 4 para. 3 sentence 3 Act on Passports (PaßG)). In Germany, since 1 November 2005 the digitised photograph of the face had previously been stored in an integrated chip in passports of the first generation.

On 1 March 2007, the Act on Telecommunications Media (TMG) entered into force. This law unites the requirements concerning telecommunications and media services from different legal bases into one single act. This includes, on the one hand, the economy-oriented rules on the implementation of the e-commerce Directive. Until that point in time, those rules had been included in the Act on Telecommunication Services (TDG) and in the so-called "Länder National Treaty on Media Services" (MDStV). On the other hand, this includes the data protection rules of the Telecommunications Data Protection Act (TDDSG) that had previously been in force and the above mentioned national treaty. The telecommunications and media services were summarised under the term "telemedia".

With regard to content, the old rules were transposed to a large extent without any modifications. This applies to those

rules that transpose the requirements of the E-commerce Directive into German law. In the data protection area, a long-standing matter of legal uncertainty has been remedied by clarifying that only the Telecommunications Data Protection Act applies for Internet access providers, providers of Internet and telecommunications services and of e-mail services. For the protection of addressees against spam, rules were established with a view to achieving greater transparency. These rules prohibit any obfuscation or concealment of the sender and the commercial character of an advertising e-mail. They also establish that any infringement will be fined.

B. Major case law

On 13 February 2007, the Federal Constitutional Court ruled that the courts have to decline the use of any covertly obtained genetic expertise on parentage as evidence due to the violation of the concerned child's right to informational self-determination. To realise the legal father's right to information about the fact whether his child is of his descent, the legislator has to provide for an appropriate procedure solely with the objective of establishing paternity (in addition to the procedure for contesting paternity). That ruling strengthens the right to informational self-determination. The balancing of interests by the court between the child's right not to disclose his data and the father's right to information whether the child is of his descent, which is protected by the Constitution, complies with the constitutional principle of proportionality. The ruling of the Federal Constitutional Court also prevents the opening of floodgates to covert genetic tests in other areas of life (e.g. insurances or employment relationships).

C.Major specific issues

As regards the fight against international terrorism, the political discussion in 2007 focused on the question as to how far police agencies and intelligence services should be granted powers to covertly conduct online searches of PCs and other information-technological systems and how pertinent legal norms related to such powers should be created.

The increasing use of the Internet when planning and carrying out terrorist activities poses new challenges to law enforcement authorities. Therefore, measures were planned in order to carry out surveillance of the Internet and to secretly intrude private PCs with the aim of discovering terrorist or criminal activities at an early stage. The North-Rhine Westphalian Act on the Protection of the Constitutional Order already contains pertinent powers for online searches for the local intelligence services.

The supporters only indicate vaguely what online searches imply exactly. It is only evident that law enforcement authorities should, by using Internet connections, intrude into computers and/or systems in order to obtain access to data stored there.

Online searches raise severe technical and constitutional questions, because nearly everybody has a PC containing extremely personal information, e.g. entries into diaries. Up to now, in particular the question remains how information, which is part of the core of private life guaranteed by the Basic Law, could be effectively protected against online access by law enforcement authorities. In the course of 2008, the Federal Constitutional Court will deal with the admissibility of covert online searches, as the rules on online searches of North-Rhine Westphalia are the subject of a pertinent constitutional complaint.

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. In 2007, Law 3625/07 amended Law 2472/97 with respect to the following:

Article 2 of Law 2472/97 was amended in order to allow the publication of cases of criminal charges or convictions. In particular, publication may be permissible, following an order by the competent Public Prosecutor of the Court of First Instance or the Chief Public Prosecutor if the case is pending before the Court of Appeal, in the case of crimes which are punished as felonies or misdemeanours with intent, and especially in the case of crimes against life, against sexual freedom, crimes involving the economic exploitation of sexual life, crimes against personal freedom, against property, against the right to property, violations of legislation regarding drugs, plotting against public order, as well as crimes against minors. The publication of criminal charges or convictions aims at the protection of the community, of minors and of vulnerable or disadvantaged groups, as well as at the facilitation of the punishment of those offences by the state.

Pursuant to the amendment of Article 3 of Law 2472/97, during the exercise by the citizens of their right to assembly, pursuant to Article 11 of the Constitution, the use of sound or image recording devices or other special technical means is allowed at the order of the public prosecution authority and if public order and security are at serious risk. The sole aim of the aforementioned recording is its use as evidence for the commission of crimes before any investigative authority, public prosecution authority or a court of law. The processing of any other material which is not necessary for achieving the aforementioned aim for the verification of committed crimes is prohibited and the relevant material shall be destroyed at the order of the competent public prosecutor.

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

Directive 2002/58/EC
Directive 2002/58/EC has been implemented into national law by 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 confusion.

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

Directive 2006/24/EC
The Standing Committee of the Ministry of Justice is currently working on a draft law by which the Directive 2006/24/EC will be implemented into national law.

Main developments
At the end of 2007, the HDPA started bringing the new information system into operation which, besides enhancing back-office functionality for the internal users, will also provide a new portal offering e-government services to the citizens.

B. Major case law

Decision 3/2007
The HDPA has ruled that the provisions of Law 2472/97 concerning the *Protection of Individuals with regard to the Processing of Personal Data* apply to the collection and processing of personal data which are collected through a CCTV system operating at a private residence that aims at or results in the monitoring of workers who offer their professional services to the household. The installation and operation of a CCTV system without the observance of the specified conditions and, in particular, without the notification of such an operation to the HDPA and without informing the data subjects is illegal and the controller is subject to the relevant sanctions.

Decision 6/2007
The publication by the Ministry of National Defence of the names of persons a) who have been legally exempt

from military service for health reasons b) who were considered exempt from military service after the supporting documents were checked for the second time c) who were illegally exempt from military service for health reasons, violates the provisions of Law 2472/97, since the above data does not fall under any of the exceptions of the law, so that the processing could be allowed.

Decision 62/07
The Hellenic Data Protection Authority issued decision 62/2007, whereby it judged that the operation of a biometric system for controlling the entrance and exit of employees, and the operation of a CCTV system in work areas is illegal. It subsequently imposed a fine of 8000 euros for the operation of the biometric system and 6000 euros for the operation of the CCTV system. The HDPA has also instructed the Data Controller to uninstall the biometric system and to follow the procedure which is stipulated in Directive 1122/2000 regarding the operation of CCTV systems.

Decision 64/07
The HDPA made a recommendation to TEIRESIAS Bank Information Systems SA and to Greek banks to establish a procedure whereby banks inform TEIRESIAS after the settlement of debts which arise from the termination of personal or consumer loans issued to natural persons by banks or financial institutions within 15 days after the settlement. TEIRESIAS shall amend its records immediately, and no later than 15 days after receiving notification about the settlement, without any further action from the data subject.

C. Major specific issues

On 19 November 2007, the President, the Deputy President and seven members of the Hellenic DPA handed in their resignation as a form of protest following the incident mentioned below:

The Data Protection Authority had issued Decision No 58/2005, whereby it allowed the use of the C4I CCTV system (293 cameras) and of 49 pre-existing cameras, solely for traffic management under particular circumstances and for the reasons referred to in detail in the decision's rationale.

In particular, it had been pointed out that the operation of the system, and the use of the data collected through the system and recorded on it, is forbidden for any other reason besides the verification of offences in accordance with the lawful use of the system and the conditions set out in the decision. The operation of cameras positioned on crossroads or road axes is prohibited when the traffic of vehicles is interrupted on them, i.e. during manifestations, demonstrations etc.

The Minister of Public Order had filed a writ of annulment against the aforementioned decision at the Council of State which was heard on 12.1.2007 and has since been pending before the Plenary Session of the Council of State. It is noteworthy that the proposal of the judge rapporteur was rejective of the writ of annulment. In addition, the Suspension Committee of the Council of State had already rejected the relevant suspension petition concerning the prohibition of the operation of cameras. In November 2007, during the pendency of this case and after a question addressed by the Hellenic Police Headquarters, the Attorney General of the Hellenic Supreme Court of Civil and Criminal Justice (Areios Pagos) issued Opinion No 14/2007 whereby the operation of the aforementioned CCTV system is allowed under the supervision of a public prosecutor in all cases, even if there is no traffic of vehicles or if the traffic of vehicles is forbidden, i.e. during manifestations, demonstrations etc., without, in any case, recording the images received, unless offences are being committed. The Hellenic Data Protection Authority, the single authority which, under the Constitution, is competent to examine this issue, in accordance with the rules for the protection of personal data, issued a press release in view of the issue that had arisen notifying that its decision, given that it had not been annulled by the Council of State, was lawful and remained, therefore, applicable and binding. Moreover, the violation of its provisions would entail administrative sanctions provided by Law 2472/97. It is for that reason that the administrative sanction of the fine had already been imposed twice on the Ministry of Public Order. Despite the explicit, categorical and unique lawful tackling of this matter on the basis of the Constitution, the aforementioned CCTV system still operated by order of the public prosecutor. Therefore, under the supervision of public prosecutors, images were received from the rally and the march which took

place on 17.11.2007, i.e. during the commemoration of the Athens Polytechnic School uprising, during which the traffic of vehicles in the area was forbidden. The said fact was confirmed by the report of the Data Protection Authority's auditors who, after receiving an order in writing, went to the Attica Police Directorate in order to carry out an audit, as provided for by the provision of Article 19, paragraph 1 of Law 2472/97. In that way, the provisions of the Hellenic Data Protection Authority's decision mentioned earlier were blatantly violated and the independence of the authority, which is safeguarded by the Constitution, was subsequently affected, while its status was diminished.

Hungary

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

Last year there was an attempt to implement Directive 2006/64/EC on the retention of data processed in connection with the provision of electronic communications services and amending Directive 2002/58/EC. The Data Protection Commissioner received several drafts in the administrative coordination procedure and made comments related to the rights to privacy, to the confidentiality of communications and to the protection of personal data. He explained that the mass retention of data does not satisfy the principles on the limitation of human rights as set down by the European Court of Human Rights, unless the limitation is necessary, adequate and proportionate to the protection of public order, national security and public safety and to ensure the prevention, investigation and fight against crimes and the illegal use of the electronic telecommunication system in a democratic constitutional state. The fight against terrorism and organised crime cannot serve as justification for every action either. The Commissioner emphasised that even if EU law provides scope for Member State legislation, automatic implementation of the high or low ends (in our case: the longest possible retention time) is unacceptable, and data protection principles must be considered. The draft has not been submitted to the Parliament.

B. Major case law

The public showed great concern about the healthcare reform which also involved the closure and integration of institutions. The Commissioner launched an *ex officio* investigation into the location of documents originally held by closed-down health institutions, as controls on the documents had an important effect on the enforcement of patients' rights to informational self-determination. The comprehensive investigation involving the concerned decision-makers and heads of closed-down institutions concluded that the institutional reform puts patients' rights to informational self-determination at serious risk because it does not resolve the control of documents held in institutions designated for closure. It can be presumed that data subjects will absolutely not be able to keep track of their medical data and documentation, which means that they will be deprived not only of their right of access to documents but of their rights provided for by the Act on Healthcare, and that institutions (doctors) providing care will not be able to obtain information on patients' medical history, which will risk the patients' ability to protect their own health, receive treatment and recover. The Data Protection Commissioner called on the Minister of Health to pay careful attention to the issue of medical documentation and to take the necessary action to ensure that all closed-down institutions consider patients' rights when deciding on the handling of medical documentation. In order to maintain proper patient care, the system of medical documentation transfers should be designed to allow continuous access to information on patient care with particular attention to non-paper based documentation as well.

One of the most important recommendations issued by the Commissioner in 2007 dealt with data protection requirements of identification in electronic administration. The recommendation discussed only the minimum criteria and did not intend to provide the only possible practical solution for identification. The objective of the document was to create framework conditions allowing clients to take care of their business efficiently while enjoying the same level of privacy as provided for by traditional administration. The principles and ideas for implementation proved to be useful guidance for electronic government, authorities and, last but not least, for citizens as well.

Messages transmitted in electronic communications, then later used in criminal proceedings, constituted a reoccurring problem in 2007. Applicable legislation views traditional mailing as the general, and electronic mailing as the exceptional way of communication, even though the later has become more popular in practice. Different rules apply to delivered traditional letters and those 'still on their way' and adequate safeguards protect data subjects from secret searches. The core of the problem is the difficulty to apply these rules to electronic mails. The 'traditional' form of electronic mailing is similar to a postal letter in that it is also communication between two specific people, the content of which is only known by the sender and recipient, the mails can be found in

their computer (system). In many cases, however, the mailing is carried out via a content provider. Data is not stored in the sender's or recipient's computer in these cases, but in the provider's computer that the sender and recipient can access through the Internet. Free e-mailing systems belong to this category as they do not perform actual data transfers.

This often results in uncertainty, like in the case of police trying to decide who qualifies as a telecommunications provider and therefore not choosing the applicable legal ground correctly. Police seizures to access data stored on the service provider's server are also a matter of concern. Application of traditional terms such as 'delivery' to a new technology or method is likely to cause difficulties. While delivery is an unambiguous term in relation to postal letters, it is ambiguous when applied to e-mails. It is simple to determine whether the recipient has viewed his mailing list or a specific e-mail, but according to the prosecutors' interpretation, it does not have significance: e-mails shall be considered delivered as soon as they have been sent. The Data Protection Commissioner informed the Chief Prosecutor that he did not agree with this interpretation and emphasised in electronic communications, the characteristics and purpose of the data flow and not its method should determine the applicability of rules on mail secrecy.

C. Major specific issues

The rules regulating data processing by law enforcement authorities were significantly amended in several points in 2007, partly as a reaction to the problems experienced during the political disturbances in 2006. The amended rules on police checks in the draft amending the Police Act are welcome, so is the reduction of excessive retention time applied to data collected during checks. However, the authorisation of police to conduct surveillance on public premises on anybody, at any time and anywhere is too general.

One of the questionable points of the bill amending certain acts in the area of criminal law is the application of electronic surveillance equipments for law enforcement purposes by penal institutions. The draft would authorise the installation of such equipment outside penal institutions as well.

It is important to mention the preparation of the new Civil Code which has been ongoing for several years and was still not concluded in 2007. The recodification of the rules on business secrets by the new draft Civil Code raises doubts. From a data protection perspective, attention should also be paid to the draft rules on the real estate register.

In 2007, we continued preparations for the accession of Hungary to the Schengen Area by checking data protection practices of Hungarian consulates issuing visas, such as the consulates in St. Petersburg, Shanghai, Hong Kong and Chisnau. The inspections focused on the necessity of collected personal data for the evaluation of visa applications and compliance of the consulates' data processing practices with data protection rules.

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. Legislative developments having a significant bearing on data protection in Ireland during 2007 included new regulations amending the designation of data controllers and data processors who are required to register with the Office. Other regulations introduced during the year provided for the designation of the processing of genetic data in relation to the employment of a person as processing that can only take place with the prior approval of the Data Protection Commissioner. From 24 October 2007, the full provisions of the Data Protection Acts have applied to all manual data.

In regard to Directive 2006/24/EC on the retention of data processed in connection with the provision of publicly available electronic communications services (amending Directive 2002/58/EC), Ireland has challenged the legal base of this Directive before the European Court of Justice. Proceedings are currently ongoing in relation to this case. Notwithstanding and without prejudice to these proceedings, this Directive (which has not yet been transposed) is expected to be transposed in early 2008.

B. Major case law

In most cases, in accordance with Section 10 of the Irish Data Protection Acts 1988 and 2003, complaints submitted to the Commissioner are resolved amicably without resort to a formal decision. Such amicable solutions may involve a donation by the relevant data controller to an appropriate charity or some similar gesture. Other strategies include more forceful use of enforcement powers when data controllers fail to respect the access rights of data subjects and a policy of naming certain data controllers in case studies included in the Commissioner's Annual Report. Nonetheless, the Commissioner made a number of individual decisions on complaints made under the terms of the Data Protection Acts. These included:

a. A decision to direct a company to cease "cold call" marketing. Following complaints of unsolicited direct marketing calls from a particular company, the Office discovered the company's marketing procedures were not sufficiently robust to uphold the data protection rights of subscribers. We accordingly instructed them to cease all "cold call" marketing until such time as the company had remedied the problem or face a legally binding enforcement notice to that effect. The company complied with our request, suspending "cold calling" for twenty days until appropriate remedial action was undertaken.
b. A decision to serve an information notice in response to a claim of legal privilege. The Office received a complaint about a data controller that failed to comply with an access request on the basis that the documents in question were privileged. Our investigation confirmed that the claim of privilege could not apply to a particular document requested by the data subject. The data controller continued, however, to claim legal privilege. The Office had no option but to serve an Information Notice requiring that a copy of the relevant document be furnished to us. On examining it, the Office was satisfied that it contained personal data related to the data subject and we were further satisfied that the limited exemptions to the right of access set down in the Data Protection Acts did not apply in this case. The document was subsequently released.

C. Major Specific Issues

In the summer of 2007, the Office undertook 'raids' of a number of companies engaged in the mobile text marketing sector. These snap inspections came in response to the large number of complaints that we received in relation to those companies and as part of a strategy to use the full powers of the Office to tackle the area of unsolicited text messages. As follow-up to the raids, we are currently bringing prosecutions against those companies that have sent or allowed to be sent unsolicited communications to subscribers or that have otherwise failed to comply with their obligations to respect the privacy of individuals.

Italy

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

Directive 95/46/EC was incorporated into national law by an act of 31 December 1996 (Act No 675) which came into force six months later. In June 2003, a new act (Data Protection Code) was adopted consolidating and totally replacing the existing legislation. This act entered into force on 1 January 2004.

Directive 2002/58/CE was incorporated into national law by the said Data Protection Code. Title X of the Code addresses "Electronic Communications" (Sections 121 to 132).

Parliamentary hearings: The authority was heard several times in 2007 on major issues addressed by the competent parliamentary committees. In particular, the authority was heard on issues dealt with by the Parliamentary committee supervising the implementation of the Schengen Agreement, Europol's activities, and immigration matters as well as taking part in the debate on the bill concerning the so-called biological will. The authority also participated in the hearings concerning bills on the setting-up of a fraud prevention system in consumer credit and regulating the TV sector during transition to digital technology. The DPA also contributed to a survey on the relationship between freedom of the press and protection of personal rights, as well as to that related to management and use of the information held by the Office of the Revenue. Reference can also be made to a hearing addressing the use of Galileo and GPS satellite navigation systems, in view of the establishment of a world satellite system for non-military purposes.

Awareness-raising in respect of Parliament and government: The tasks conferred on the Italian DPA based on the DP Code include calling Parliament's and the government's attention to the advisability of regulating certain sectors. In this connection, Italy's government submitted a proposal to Parliament to set up a DNA database managed by police for security reasons. We had the opportunity to draw Parliament's and the government's attention to the need for setting out some fundamental safeguards in view of the establishment of this national DNA database. In particular, the authority specified that this database should only be aimed at the identification of individual persons. Consequently, the mandatory collection of DNA samples must not be envisaged – and where envisaged in respect of certain categories such as persons arrested, investigated, indicted and/or sentenced, proportionate safeguards must be set out; on the other hand the retention period of identification data should be proportionate to the purposes. Additional safeguards were laid down in respect of access mechanisms (access logging was recommended) and the exercise of data subjects' rights. A similar exercise related to the parliamentary debate on a bill whereby SMEs and self-employed professionals would have been exempted from the application of minimum security measures. The bill would have considerably reduced the safeguards applying to processing of employees' data by a large portion of Italian businesses. The DPA pointed out that Community and international legislation did not allow exempting a whole category from the application of substantive regulations in terms of personal data protection – as well as giving rise to discrepancies compared to the processing operations performed by public bodies. Additionally, the Italian DPA called upon the Italian Parliament to introduce amendments to the Data Protection Code to allow considering additional tools (in particular, binding corporate rules) to provide adequate data protection under the terms of the European Directive (Article 26(2)).

Opinions: Under the DP Code, the Italian DPA is to be consulted by the Prime Minister and each Ministry whenever regulations and administrative instruments are to be issued that are liable to impact on data protection matters. In 2007, this took place several times; in particular, reference can be made to the opinions concerning the computerised register of car taxes; membership and tasks of the Committee in charge of international adoptions (here we allowed the processing of personal data related to foreign children that are adopted by or placed under the custody of Italian parents exclusively with regard to indispensable data and in compliance with the safeguards laid down in the DP Code); use of the financial system for the purpose of laundering criminal proceeds and the financing of terrorism; the technical rules on ID cards and electronic IDs; coordination

of public administrative activities aimed at protecting minors against sexual exploitation and misuse; the provisions regulating payments by public administrative bodies; the self-regulation code applying to media and sports; and the mechanisms to enable local authorities to participate in tax controls and other arrangements aimed at countering tax evasion.

B. Major case law

The Italian Court of Cassation (Supreme Court) issued several decisions related to data protection in 2007:

Territorial jurisdiction on data protection: The Data Protection Code provides that the court of the place where the data controller is resident is territorially competent for any litigations related to application of the provisions set out therein. Such competence may not be derogated from.

Access to employees' e-mails: Accessing another's correspondence is punishable if the correspondence in question is "sealed". As for the correspondence sent via computer networks, it is "sealed" vis-à-vis any entity that is not authorised to access the IT systems used for sending/receiving the individual messages. In particular, it was ruled that the correspondence stored in a company's IT system could be lawfully accessed by any entity (including the employer) holding, on lawful grounds, the relevant access keys (user ID + password); instructions and information to that effect had been issued by the company to all employees to enable access in case the individual user was absent. This is in line with the guidance provided by the Italian DPA in a decision dated 1 March 2007 (see below), whereby corporate senior staff may lawfully access the computers/IT devices made available to employees if the conditions legitimating such access have been notified in full to the employees in question. Conversely, as ruled by the court in another decision, a company's system administrator may not access employees' emails by using the privileges (in IT terms) vested in him – such as the possibility to allocate passwords to email account holders. The latter are unquestionably free to replace the administrator-assigned passwords by other passwords of their choice, to protect confidentiality and privacy, and the administrator is not entitled to access the individual accounts thereafter. The court pointed out that the fraudulent interception of communications did not consist in performing the interception so as to make it impossible or extremely difficult to detect the intercepting entity, but rather in performing interception so as to override and/or dodge the security mechanisms deployed to prevent third parties from accessing the communications at issue.

Freedom of the press and confidentiality of sources: An order issued by a judicial authority in Rome to seize the computer used by a journalist was quashed by the Court *inter alia* because it failed to take account of professional secrecy and the privileges applying to journalists. According to the court, special care is necessary in applying measures such as search or seizure to journalists because of the potential limitations this might bring about in respect of freedom of the press. In particular, journalists' professional secrecy is meant to safeguard freedom and impartiality of the press and is not a privilege granted to the individual journalist.

Videophones and child pornography: Disseminating a pornographic video (showing the sexual intercourse between a young girl and other boys) via cell phones meets the legal definition of child pornography. In the court's view, the criminal offence in question is established under Italian law to punish not only the commercial exploitation of child pornography, but also any type of conduct that may give rise to pornographic materials involving minors. The defendant had recorded and disseminated (via his cell phone) a video showing a young girl having sexual intercourse with several boys, and this was an instance of child pornography because it could be easily foreseen that the materials in question were bound to be disseminated further by the initial recipients – thereby enhancing their prejudicial effects, in particular with regard to the victim's life and personality.

Reference can also be made here to *a decision by the Council of State* (last instance judicial authority for administrative law disputes), which ruled that it was lawful to record a conversation without informing the counterparts in order to use the recording as evidence in a trial. In the judges' view, no disciplinary sanction was to be imposed on a university professor who had recorded

his conversations with other teachers and students in order to obtain evidence that could be lawfully used in a judicial proceeding – as this would be tantamount to punishing an activity that consists in the legitimate exercise of the right to establish and defend a judicial claim.

C. Major specific issues

Law enforcement databases

The management of large databases for law enforcement purposes was one of the main focuses of attention for the Italian DPA also in 2007. In particular, the authority also carried out in-depth investigations in respect of the processing of data by judicial offices. The need for applying more stringent security measures in this sector was pointed out – in particular with regard to the exchanges of wiretapping records between telephone operators and judicial authorities. The lack of adequate arrangements in respect of the keeping and handling of personal information was confirmed, *inter alia*, by the inspections carried out at the Court of Rome, the largest one in Italy in terms of the number of cases handled annually. The authority continued its cooperation with the Ministry of Justice, the National Council of the Judicature, and judicial authorities in order to enforce and facilitate compliance; the lack of sufficient financial resources should be referred to here as one of the main reasons for the difficulties encountered by the judicial sector in ensuring adequate safeguards to citizens' data.

Security in telephone and electronic communications

Following an in-depth investigation into the processing of personal data by the main telecommunication operators in Italy, the authority discovered abnormalities in the collection and processing of personal data related to use of the Internet. In particular, some operators acting as "internet access providers" were keeping detailed records of their users'/subscribers' web navigation, allegedly because they were obliged to do so by the law. To that end, various tools were used including hardware probes, transparent proxies and packet inspection techniques, which allowed collecting information with a detail level ranging from the source/destination IP address couple to fine-grained HTTP logs – up to search engine query strings submitted by users, authentication credentials transmitted over simple HTTP connections and any sensitive information that can be specified in an URL format web address. This kind of processing is not justified by technical reasons as related to the tasks discharged by Internet access providers, which is why the authority issued three provisions to ban the processing in question and ordered the providers to delete all the users'/subscribers' navigation data recorded unlawfully within sixty days. The Italian DPA also adopted a general provision regarding the storage and processing of traffic data produced by telephone and internet service providers. This was aimed at ensuring enhanced security in respect of the traffic data retained by providers for lawful reasons (including law enforcement purposes). The measures developed by the Garante clarify who is to retain which data and lay down technical and organisational arrangements to ensure secure storage of the data in question. In particular, it is clarified that Internet content providers, search engine managers, public bodies/organisations making available telephone and Internet networks to their staff and/or using servers made available by other entities, Internet cafés and similar establishments fall outside the scope of application of the retention obligations at issue – pursuant to the definitions set out in Directive 2002/22/EC on universal service as well as in Directives 2002/58/EC and 2006/24/EC. Several technical measures were set out in order to protect the data – including strong authentication and biometrics procedures, fine-grained audit applied to databases and computer systems, encryption of databases, centralised and securitised log collection, and physical security measures for the protection of computer rooms and data centres.

Formal complaints

In 2007, there were 316 decisions on formal complaints. Like in previous years, most of these concerned banks, financial companies and credit reference agencies. A few cases related to processing of the so-called commercial information (assets and liabilities, bankruptcy/winding-up procedures, etc.) by companies operating in this sector; they resulted into decisions urging such companies to perform in-depth checks before re-using public information in order to ensure that the information in question was updated, accurate, and complete.

Several cases that addressed the processing of data for journalistic purposes enabled the DPA to probe deeper into the "personal data" concept. Regarding identifiability of data subjects, the data related to individuals who were not explicitly identified but could be recognised by reference to other items of information held by the data controller (or available elsewhere) was considered to be personal data; however, it was stressed that it was necessary to take account of all the means that could be reasonably used by the data controller and/or another entity to identify the person in question. Mention should also be made of a case in which the personal information published in respect of two individuals other than the complainant – whose husband had been reported to have deceased in a car accident while he was "with his current partner" – was considered to be personal data related, albeit indirectly, to the said complainant because it produced effects that also impacted on the complainant in question.

Interestingly, the DPA ruled that the complaint lodged against a hospital was inadmissible because the access request was not aimed at obtaining communication of personal genetic data held by the hospital, but rather the delivery of a tissue sample related to the complainant's deceased father (in particular, a "tissue fragment included in paraffin" and/or a blood sample.)

Inspections

The inspection activities by the Garante were enhanced in 2007, partly on the basis of the six-month inspection plans developed by the DPA. 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. Overall, 452 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 (medical) data by pharmaceutical companies and healthcare bodies; the online processing of personal data; processing aimed at the provision of goods and services via distance selling mechanisms (including call centres); the processing operations performed by Revenue Offices; the retention of users'/subscribers' data by telecom operators; and e-banking services.

Following the inspections, 228 proceedings were instituted with a view to the imposition of administrative sanctions; in 15 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 to about 725,000 euro.

Mention should also be made of the specific activities carried out by the Italian DPA in pursuance of international agreements and conventions, especially those related to operation of the Schengen Information System and Eurodac databases.

Public sector

Biometrics. The DPA authorised a public body (office of the Superintendant for Archaeological Heritage) to use the hand contour in order to enable employees to access a high-security area. The biometrics-based system to be deployed by the office will only rely on the geometric features of the employees' hands without including any other biometric data. The hand contour will be associated with an encryption algorithm and stored in the internal memory of the biometric equipment; the latter will only be operating in local mode by means of a digital keyword to be selected and entered by the individual employee. This processing was found by the DPA to be lawful and proportionate; whilst the hand contour information does not enable unique identification as is the case, for instance, with fingerprints, it is sufficiently detailed to be used in specific situations with a view to identity controls.

Employment issues. Guidelines were issued in respect of the processing of employees' personal data in the public sector. The guidelines address the processing of public employees' medical data; the collection of fingerprints to access the workplace; and the dissemination of data on the Internet.

Local authorities. The DPA issued guidelines on the processing of personal data with a view to the publishing

and dissemination of documents by local authorities. Specific safeguards were laid down in respect of the data related to individuals mentioned, e.g. in decisions and resolutions posted on the municipal bulletin board, in publicly available documents and/or in documents posted on the Internet, so as to take due account of the principle of transparency.

Schools. The DPA clarified that parents may film and take pictures of their children on the occasion of school theatricals, as the images in question are not intended for dissemination and are collected for personal purposes in order to be circulated among family members and friends. The DPA also provided guidance, in co-operation with the Ministry for Education, on the use of videophones by students/pupils in schools.

Healthcare

- The Italian DPA instructed local healthcare agencies not to include medical diagnosis information in the disability certificates they are required to issue for the applicants to be enrolled in unemployment lists and/or exempted from the payment of school/university taxes.
- Dissemination on the website of an Italian region of the names related to 4,500 patients as well as of information on the respective health status was prohibited by the DPA.
- It was clarified that local municipal authorities may not request physicians to provide names and/or other items of information to identify the patients they visit at home.
- An inspection was ordered by the DPA and carried out with the help of the Financial Police following media reports on the presence of hundreds of medical records in a garbage dump. Information was preferred to judicial authorities against the relevant data controllers because of their failure to take minimum security measures.
- The DPA urged a public body to use payment order forms containing no references to the diseases affecting the respective beneficiaries, in particular HIV-related conditions; the inclusion of general wording and/or numerical codes was recommended.
- A leaflet was published and disseminated ("Protecting Personal Data: Siding with the Patient") to raise citizens' awareness of the importance of data protection in processing operations performed by medical staff, healthcare bodies, and/or medical labs. It contains concise information on patients' data protection rights and the mechanisms to enforce them.

Processing of genetic data

Genetic data may only be processed in the cases provided for by *ad hoc* authorisations granted by the Garante (after having consulted with the Minister for Health who shall seek, to that end, the opinion of the Higher Council for Healthcare) and, as a rule, with the data subject's written consent.

The general authorisation issued by the Garante in February 2007 to enable this kind of processing filled in a major gap in the regulatory framework. It applies to several categories of data controller for purposes mainly consisting in the provision of healthcare and the performance of scientific research activities; the issue of genetic data used for facilitating family reunion was also tackled.

After defining the main concepts (genetic data, biological sample, genetic test), the authorisation lists the entities authorised to process genetic data for the purposes specified in the individual cases (healthcare practitioners, public and private healthcare bodies, medical genetics laboratories, natural and/or legal persons for scientific research purposes). The principle whereby genetic data may only be processed for such purposes if it is actually indispensable was re-affirmed along with the need for obtaining the data subject's written consent – the only exception being where genetic data is necessary to safeguard the genetic identity (with a view to reproductive choices, or treatment) of a third party belonging to the same genetic line as the data subject and consent may not be provided on specific grounds (legal incapacity, physical impairment, mental disability), or where statistical surveys are at issue or the research activity is provided for by law.

Data controllers must fulfil specific obligations, which are especially stringent as regards the contents of information notices. Genetic counselling is a mandatory requirement if the data is processed for healthcare or family reunion purposes, both before and during the genetic testing. Specific processing arrangements

must be complied with and stringent security measures adopted – including encrypted storage and communication of genetic data and separation of identification from genetic data. The retention period of the data in question must not exceed what is absolutely indispensable for the specific purposes; no genetic data may be disseminated.

Private sector

A major effort was made by the Italian DPA in 2007 in order to simplify application of data protection legislation in the private sector.

Bulk debt transfers and securitisation

A decision (published in Italy's Official Journal of Laws and Regulations) allowed dealing with several applications lodged with the DPA for exempting data controllers from the obligation to provide information to data subjects in connection with bulk debt transfer and/or securitisation. Such operations entail disclosure by the transferor to the transferee of personal data related to the debtors. Under the DP Code, the data controller may be exempted by the DPA from information obligations in specific cases, providing the processing at issue is publicised adequately – according to mechanisms to be set out by the DPA. The Italian DPA ruled that providing information to the individual data subjects (the debtors) entailed a disproportionate effort in this case and exempted the data controllers from the relevant obligations on two conditions: namely, an exhaustive information notice was to be published in the Official Journal no later than when the transfer took effect, and the debtors were to be provided with individual notices on the first useful occasion following the transfer (e.g. when sending the bank statement, or making a payment request) so as to inform them that the transferee had collected their personal data from third parties.

Guidelines for the monitoring of e-mail and Internet usage

The DPA issued a general decision (dated 1 March 2007) applying to the monitoring of e-mail and the Internet carried out by public and private employers alike – in the light both of the case law of the EHRC (case of Copland v. UK) and the stance taken by the WP 29. Pursuant to Italy's constitutional framework, employers are required to afford reasonable privacy to their employees in order to ensure that their personality can develop freely and without constraints. Given these assumptions, the guidelines in question attempted to reconcile the interests at stake by re-affirming, on the one hand, the employer's right to lay down the usage arrangements for the IT equipment committed to employees – including proportionate disciplinary measures – and, on the other hand, employees' right to be the subject of controls carried out in a stepwise, proportionate manner and be adequately informed about the processing of their data, which must be minimised. Specific recommendations and prohibitions were laid down in this framework – among the former, the need for employers to adopt an in-house policy tailored to the dimensions of the enterprise, and adequately inform their employees about the mechanisms for using email, the Internet and other electronic tools by also specifying whether and to what extent controls are carried out; as regards specifically the Internet, the categories of website considered relevant to the employment context should be specified, and configuration mechanisms and/or filters should be deployed to prevent certain operations (e.g. certain downloads); additionally, shared email accounts should be made available as well as an *ad hoc* email account to allow receiving personal correspondence, whilst employees should be invited to designate a trusted third party (e.g. another employee) to access their mail and forward relevant messages in case they are away from work. The authority prohibited any activity on the employer's part aimed at performing remote monitoring of employees; where such monitoring requirements are related to production, organisation and/or security in the workplace, the agreement of trade unions should be sought as provided for in other pieces of legislation. Based on the balancing of the interests at stake, the authority decided that monitoring for preventative purposes may be carried out without the employee's consent also at an early stage, i.e. irrespective of the existence and/or the planned institution of litigation, providing all the safeguards specified above are in place and the monitoring is proportionate to the specific context (e.g. on account of security risks).

Simplified mechanisms to ensure data protection in the insurance sector

The Italian DPA authorised insurance companies to implement a new, simplified procedure in order to inform customers of the processing of their personal

data. Account was taken in this regard of the experience gathered over the past few years within the framework of the so-called "insurance chain", which includes several stakeholders such as joint insurers and re-insurance companies. In practice, it was decided that the information notice will have to be provided once and for all by the insurance company stipulating the contract with the individual customer. That company will be responsible for informing the customer about any subsequent and/or further use of his/her personal data – including the respective purposes and recipients – also on behalf of other entities in the "insurance chain", who often have no direct contacts with the data subjects even though they may process personal information after collecting it from the insurance company. Specific safeguards were laid down by the DPA in order to enable the companies to avail themselves of these simplified information mechanisms – in particular, the insurance company will have to inform customers about the entities processing their data in connection with the specific contracts; an updated list of those entities will have to be posted on the company's website, partly in order to facilitate exercise of access rights by data subjects; any purposes pursued by the companies/entities in question other than those related to risk management will have to be specified in the information notice; and specific consent requirements will have to be complied with whenever consent is actually necessary – which is often not the case, e.g. because the customer's data is indispensable to stipulate and/or enforce the contract. In particular, it was recalled that processing customers' data for marketing purposes requires *ad hoc* consent, and that sensitive data (including medical information) may only be processed by insurance companies with the customers' written consent.

Practical guidelines for SMEs

Practical guidelines were issued to take account of the specific needs applying to SMEs in respect of data protection issues. Starting from the consideration that certain requirements under personal data legislation are sometimes considered burdensome, in particular by SMEs, and in order to foster the view that data protection can turn into a major business asset as it can increase consumers' and users' trust, the Italian DPA issued the guidelines in question to provide SMEs with a tool that can facilitate compliance and highlight the simplification measures that are currently available. As well as clarifying the main obligations that apply to any entity processing personal data and basic data protection concepts (data controller/data processor; information notice; consent and mechanisms for ensuring it is informed, in particular when sensitive data is to be processed), the guidelines clearly set out in which cases the processing is to be notified to the Italian DPA and what security measures a company performing standard business activities is required to take. The options currently available for cross-border data flows were also described, including the use of standard contractual clauses and a checklist was made available so as to enable a company to verify whether all the relevant steps were taken in view of ensuring compliance.

Use of customers' data by call centres and telecom operators (inbound and outbound services)

Following in-depth inspections carried out all over Italy (with the help of the Financial Police) in respect of the main telephone operators and call centres, it could be established that personal data had been processed unlawfully in several cases and unfair processing practices had been put in place. The Garante issued five decisions in June 2007 setting out measures to be implemented by some of the most important telephone operators and call centres in order to comply with privacy and other rights vested in users. The decisions in question required phone companies and call centres handling outbound services to terminate all unlawful data processing operations (in particular to activate unsolicited services such as high-speed Internet connections) and inform the Garante on the steps taken to implement the organisational, technical, and procedural measures set out therein (providing information notices to users and obtaining their specific consent to the use of data for advertising purposes; ensuring transparency when first contacting users as to the source of the respective data and the mechanisms of their use; taking note of a user's objection to further contacts; checking on the activity carried out by call centres appointed as data processors.) In case of non-compliance, the Garante reserved the right to issue more stringent provisions such as blocking or prohibiting processing operations.

With specific regard to inbound services, simplified arrangements were laid down in December 2007, partly based on the outcome of the inspections carried out to verify compliance with the above decisions. It was clarified that call centres handling inbound customer calls are not required to inform customers in respect of personal data processing operations, unless the data collected by the operator taking the call are to be used for different purposes (e.g. marketing) – in which case the data subject's informed consent will have to be obtained.

Media

Several issues were addressed in 2007 concerning data protection and journalism. As for the so-called court journalism, the DPA found that publication by some media of the transcripts (including wiretapping transcripts) from ongoing judicial investigations was in breach of DP legislation – in particular, because the transcripts contained personal data (some of them relating to sex life) and their dissemination was in breach of the principle whereby the published information must be "material in view of the public interest". This principle is actually also laid down in the Code of Practice for the processing of personal data by journalists. In other cases it was found that personal data had been collected in breach of fairness and lawfulness principles – e.g. because pictures had been taken intrusively, or because videos had been recorded unbeknownst to the data subjects; of note, the processing in question was also in breach of the fairness and transparency obligations set out in the journalists' Code of Practice mentioned above. In a case concerning publication of news reports on a lady deceased after a serious illness, in which excessive identifying information had been disclosed, the DPA found that the safeguards set out both in the DP Code and in the journalists' Code of Practice had been violated since they apply to the deceased as well. Reference should be made finally to the special protection afforded to children by the DP Code in connection with media and journalism; a code of practice (Charter of Treviso) was adopted a few years ago for this purpose by the Italian Journalists' Association and endorsed by the Italian DPA. Many cases concerned the publication of data that allowed identifying – unnecessarily – children involved in legal disputes (separation, divorce) and/or in criminal proceedings related to sexual abuse.

Latvia

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

Directive 95/46/EC is transposed into national law by the Personal Data Protection Law that came into force on 20 April 2000, last amendments in 2007. In order to ensure complete independence of the Data State Inspectorate of Latvia, a draft law on the Data State Inspectorate has been elaborated and is to be submitted to the government by mid-2008.

Amendments to the Personal Data Protection Law
Personal Data Protection Law was amended on 1 March 2007 and the aim of these amendments was to determine exemptions from the obligation of notification and to simplify the procedure of notification of personal data processing:

1. the exemptions to the notification have been determined;
2. instead of personal data processing systems the data controllers are being notified;
3. establishment of personal data protection officer institution;
4. the order for personal data transfers to the third countries has been specified and in regard to that the draft regulations of the Cabinet of Ministers have been elaborated.

Regulations issued by the Cabinet of Ministers
Regarding the amendments to the Personal Data Protection Law, the Data State Inspectorate of Latvia has drawn up several drafts of the regulations of the Cabinet of Ministers:

- Accreditation of personal data auditors;
- Amendments to the mandatory organisational and technical requirements for personal data protection;
- Order of the data protection officers' training;
- Standard requirements for agreements for personal data transfer to third countries.

Amendments to the Criminal Law
In order to facilitate the protection of personal data processing and to prevent illegal personal data processing, the work on stipulating criminal liability for violations in the processing of personal data was commenced. The draft amendments were submitted to the Parliament in 2007.

The draft law stipulates criminal liability for illegal personal data processing if significant harm has been done and if processing has been performed in order to take vengeance, blackmail or with other intentions, or if it is connected with violence, fraud or threats; for not using the required technical and organisational means to protect personal data and prevent illegal processing thereof due to which substantial damage has been incurred, and for illegal processing of personal data due to which substantial damage has been incurred.

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

Regulations on data retention for law enforcement purposes
Directive 2002/58/EC is transposed into national law by the Electronic Communications Law.

In relation to this issue, the Cabinet of Ministers on 4 December 2007 issued Regulations No 820 "Order on the information requests from the pre-trial investigation institutions, subjects of the investigation actions, state security institutions, prosecutors and courts and on the provision of retention data by the electronic communication service providers, as well as the order on how to summarise the statistical information on the requested retention data and how to submit it". Since 2007, the Data State Inspectorate has been the responsible authority for summarising the statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network that has been processed by electronic communication service providers in accordance with Article 19 of the Electronic Communication Law and Article 10 of the 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 amending Directive 2002/58/EC*.

B. Major case law

In 2007, the major complaints received by the Data State Inspectorate on the violations of the Personal Data

Protection Law were related to personal data processing without any legal basis.

Most common violations of personal data processing:
1. incorrect and often explicitly illegal personal data processing in the collection process of loans (credit) and payments overdue (black lists), and publication of personal data of house maintenance services;
2. violation of data subject rights on access to information – information not provided to data subjects and refusal to provide it, including non-informing about video surveillance;
3. violation of the principle of proportionality in personal data processing, exceeding and expanding the initial purpose of data processing, as well as copying of passports.

C. Major specific issues

The Data State Inspectorate received 120 complaints in 2007. As a result of inspections in the personal data protection field in 2007, violations of the Personal Data Protection Law were determined in 30 cases. Mostly the complaints concerned data processing without a legal basis, making up 50% of violations in 2007, as well as the violation of the data subject's rights (Article 10 and 11 of Directive 95/46/EC) and the violation of the proportionality principle in data processing.

None of the decisions of the Data State Inspectorate have been repealed by the court. All the appeals have been dismissed.

Supervision of SPAM

In accordance with the Information Society Services Law, since 1 June 2007 the Data State Inspectorate has been the supervisor of SPAM concerning violations with regard to personal data protection.

The Data State Inspectorate issued the first decision regarding the prohibition of sending unsolicited commercial communications (Article 13 of Directive 2002/58/EC).

Freedom of information and data protection

There was a discussion on the availability of the information concerning the fitting and the maintenance work carried out by a state agency on the flat of the former president of Latvia. This flat would be at the disposal of the former president after her term of office.
The opinion of the Data State Inspectorate was that since the fitting and maintenance work was carried out using the state budget, the information on how much the state agency spent on this purpose and should not be determined as restricted access information.

There was a case related to a magazine which made some sensitive health data (roentgenogram) public. The Data State Inspectorate took a decision that sensitive medical data should not be published at the "Yellow Press Magazine" without the consent of the data subject, and this magazine had violated the Personal Data Protection Law and the Law on Press and Media which prohibits the publication of health data in the media.

Schengen Information System (SIS)

Before Latvia joined the Schengen Zone in December 2007, the Data State Inspectorate carried out inspections of institutions and authorities which would have access to the Schengen Information System (SIS). The readiness of these institutions was evaluated, and discussions were held on how to ensure data subjects' rights regarding access to SIS.

In 2007, the law on SIS came into force which encompasses the requirements regarding personal data protection. The Data State Inspectorate also took part in the drawing up of the regulations of the Cabinet of Ministers concerning personal data processing and data subjects' right to request information collected about him or her or that his or her personal data be supplemented, rectified or deleted from the SIS.

The Data State Inspectorate produced a brochure entitled "Personal Data in Schengen Information System". A similar brochure was produced in English and Russian in cooperation with the Slovenian Information Commissioner's office.

Research of specific fields regarding data protection

The Data State Inspectorate organised seminars regarding data protection in schools – one for the directors of schools and the other for teachers. As a result of this activity, the Data State Inspectorate has decided to make data protection in schools its research priority in 2008.

Lithuania

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

1. On 19 December 2006, the Seimas of the Republic of Lithuania (the Parliament) adopted an amendment to the Law on Documents and Archives (entered into force on 11 January 2007), under which access to the documents of the special part of the National Documentary Fund shall not be limited. The special part of the National Documentary Fund shall consist of the activity documents of the structures of the opposition (resistance) to the occupation regimes of the USSR and Germany, the People's Commissariat for Internal Affairs of the Lithuanian SSR (from 1940 to 1941 and from 1944 to 1946), the People's Commissariat for State Security of the Lithuanian SSR (in 1941 and from 1944 to 1946), the Ministry for State Security of the Lithuanian SSR (from 1946 to 1953), the Ministry of Internal Affairs of the Lithuanian SSR (from 1946 to 1954), the Committee for State Security of the Lithuanian SSR (from 1954 to 1991), the People's Commissariat for State Security of the USSR (NKGB), the Ministry for State Security of the USSR (MGB), the subdivisions of the Committee for State Security of the USSR (KGB), which operated in Lithuania from 1940 to 1991, the subdivisions of the People's Commissariat for Internal Affairs of the USSR (NKVD) and the Ministry of Internal Affairs of the USSR (MVD) which operated in Lithuania from 1946 to 1954, the subdivisions of the People's Commissariat of Defence of the USSR (NKO) and the People's Commissariat (Ministry) of the Navy (NKVMF) which operated in Lithuania in 1941, from 1943 to 1946, the subdivisions of the Main Intelligence Directorate of the General Staff of the Soviet Army (GRU) which operated in Lithuania from 1940 to 1991, the Communist Party of Lithuania as well as structures subordinate to these organisations. A person who wishes to familiarise himself with the documents must apply to the document holder, submitting a written request and a document proving his identity. A person should not be obliged to give reasons for having access to documents. A person may only access documents on the premises of the document holder. The amendment to this law also establishes that access to the documents containing information regarding persons who have admitted to secret collaboration with the intelligence agencies of the USSR and who have been entered in the records of persons confessing to this, as well as in cases when a person who suffered at the hands of the intelligence agencies of the USSR, express their wish for the limitation of use of the information on them until their death, shall be limited.

2. On 3 April 2007, the Seimas of the Republic of Lithuania adopted an amendment to the Law on the Residents' Register, which establishes that relationship and relationship by affinity (sister-in-law, brother-in-law) data, on single occasions and specifying the purpose of data use, may be provided to law enforcement personnel for the discharge of determined duties and to the Seimas Commissions for the implementation of tasks entitled by the procedure laid down in the laws, Seimas resolutions. It was also established that the data relating to the relationship may be provided to the Chief Official Ethics Commission for discharging its direct functions; notaries – for handling inheritance cases and identifying whether there are any legal provisions which restrict the conclusion of agreements between close relatives of the deceased; to persons having the right assigned to them by law to consider issues pertaining to the citizenship of the Republic of Lithuania for decision-making on these issues.

3. The State Data Protection Inspectorate issued sample Rules for Personal Data Processing at Schools, which were approved by the Order No 1T-45 of 4 July 2007 of the Inspectorate Director. The aim of Rules for Personal Data Processing at Schools – to regulate personal data processing at school in order to ensure the compliance and implementation of the Law on Legal Protection of Personal Data of the Republic of Lithuania as well as other laws and legal acts governing the processing and protection of personal data.

B. Major case law

Genealogical tree

Upon handling a personal complaint, the State Data Protection Inspectorate found that police officers, upon detaining the claimant for contravening traffic regulations and in order to reveal the claimant's identity, checked his personal data and composed his genealogical tree. Data relating to the claimant's relationship

were printed and attached to the case of administrative law violation as evidence that the offence of administrative law has been committed by him. The State Data Protection Inspectorate issued an instruction to the Police Department demanding the revocation of the measure concerning software enabling (granting the right) the combination of personal data available on the Residents' Register and the construction of individuals' genealogical trees, because the online search tool functions are legally unsubstantiated, therefore being in contravention of Article 3, Part 1 (2) of the Law on Legal Protection of Personal Data of the Republic of Lithuania.

The Police Department appealed against the instruction issued by the State Data Protection Inspectorate, claiming that the online search software tool is needed for carrying out the tasks assigned by the Law on Police Activities of the Republic of Lithuania, and for the implementation of provisions specified by the Law on Organised Crime Prevention, the Law on Operational Activities, the Law on the Control of Arms and Ammunition of the Republic of Lithuania.

Vilnius District Administrative Court concluded that the use of such software complies with the criteria for lawful processing of personal data established by Article 5, Part 1(6) of the Law on Legal Protection of Personal Data of the Republic of Lithuania. In this case the software enabling the combination of data from the Residents' Register and composition of individual's genealogical trees was needed for the pursuit of legitimate interests, for the police to carry out the tasks assigned to them by law, and in this case it was acknowledged that the data subject's interests were not overriding. A court issued a decision to repeal the instruction issued by the State Data Protection Inspectorate.

The decision of Vilnius District Administrative Court was appealed against at the Supreme Administrative Court of Lithuania.

The Supreme Administrative Court of Lithuania concluded that the Police Department had not only been collecting and processing personal data, but that individuals' genealogical trees had also been included in the database of Road Traffic Offences. Data had been collected and processed relating not only to the offender of traffic regulations and his family members, but also relatives of individuals' grandparents, uncles, aunts, brothers, sisters, cousins and also children of cousins. A retention period for these data had not been set. No legal act specifies that the genealogical tree of offenders of traffic regulations should or may be composed in the database of Road Traffic Offences. Data subjects remain unaware of this sort of personal data processing. The court concluded that in composing the genealogical tree of individuals as offenders of traffic regulations the processing of personal data involves data processing of a number of other persons, which is not related to the committed road traffic offence and bears no relevance to the provisions laid down by Article 5(1) of the Law on Police Activities of the Republic of Lithuania, Article 7, Part 1 (11) of the Law on Operational Activities or Article 17, Part 1 (9) of the Law on the Control of Arms and Ammunition of the Republic of Lithuania. This data, upon composition of the individual's genealogical tree, could be processed only for the person under operational investigation, but not for the person, who contravened Road Traffic Regulations. The court acknowledged the instruction issued by the State Data Protection Inspectorate as valid.

Bank's documents in garbage bags

The State Data Protection Inspectorate received information by e-mail that bank documents containing personal data and copies of documents certifying identity were found in garbage bags near a bank.

After an inspection carried out at the bank on the lawfulness of processing personal data, it was revealed that the documents in the garbage bags found in the proximity of the bank were not properly destroyed nor were copies of documents containing personal data. The documents and the copies of documents were destroyed in a manner allowing the identification of personal information and a natural person could be identified from the personal data remaining in the parts of the documents and the copies of documents. Upon inspection it was established that the bank, following the requirements determined by Article 24(1) of the Law on Legal Protection of Personal Data of the Republic of Lithuania, had implemented the appropriate organisational and technical measures intended for

the protection of personal data against any accidental or unlawful destruction, alteration, disclosure as well as against any other unlawful processing. However bank employees X, in the course of processing personal data, i.e. when destroying the documents and the copies of documents containing personal data not necessary for further work, destroyed them in a manner whereby the personal information remained identifiable and the personal data, due to improper destruction of documents and the copies of documents containing personal data thrown out in garbage boxes, became accessible to third persons, and that the personal data remaining in the parts of the destroyed documents and the copies of documents could identify natural persons, to whom the said documents belonged without having legal grounds for this under the Law on Legal Protection of Personal Data of the Republic of Lithuania or any other legal act. The employees X of the bank in processing personal data did not keep the personal data confidential and violated Article 24(5) of the Law on Legal Protection of Personal Data of the Republic of Lithuania. Bank employees X were issued protocols on administrative offences for the determined administrative violations. The rulings of the Court of First Instance acknowledged that the bank's employees X committed the administrative offences.

C. Major specific issues

Personal data processing for the purposes of election campaigning

During the 2007 election campaign to municipal councils, a number of indignant voters contacted the State Data Protection Inspectorate claiming that, during the election campaign, voters had been sent letters urging them to vote in support of the party or nominated candidate who had sent the letter. Responding to these complaints, the State Data Protection Inspectorate carried out an inspection of the lawfulness of processing personal data for the purposes of election campaigns and of data indicated in general electoral rolls, in parties, political organisations, and unions.

The Law on Elections to Municipal Councils of the Republic of Lithuania foresees that parties, which are registered in the State Register of Personal Data Controllers, may obtain general electoral rolls (in electronic storage media or printed) which specify: voters' names, surnames, addresses and dates of birth. If a voter, in the manner prescribed by legal acts, has expressed his disagreement that his address or date of birth should be made public in general electoral rolls, only his name and surname shall be indicated in these rolls. This law also establishes that parties may not submit general electoral rolls to the third persons or use them for purposes other than campaigning. They must destroy the obtained data within 30 days of the proclamation of the final election results.

Eight parties were included in the State Register of Personal Data Controllers which intended to process voters' personal data for the purpose of election campaigning. In the course of the inspections, it was revealed that two parties of the registered eight did not avail themselves of the opportunity to obtain general electoral rolls. Six parties received the rolls, although only four sent personalised campaign letters to electors.

Breaches of the Law on Legal Protection of Personal Data of the Republic of Lithuania were only found in one party out of six. Various violations of the Law on Legal Protection of Personal Data of the Republic of Lithuania were identified in the other five parties: not documented regulations for organisational and technical measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, disclosure, as well as against any other unlawful processing; not ensuring that personal data was being processed only by authorised persons and that these persons were not instructed in writing to keep the personal data confidential; precise information regarding the processing of personal data was not submitted to the State Data Protection Inspectorate; proper data processors were not selected and they were not properly authorised to process personal data; personal data security was not ensured appropriate technical measures for data protection were not ensured the adequate destruction of all personal data submitted to data processors was not ensured. The parties were issued the instructions on the identified violations of the Law on Legal Protection of Personal Data of the Republic of Lithuania.

Investigations at shopping centres on the processing of video surveillance data

The State Data Protection Inspectorate, on its own initiative, carried out investigations in four supermarkets regarding the scope and lawfulness of video surveillance

data processing. Violations of the Law on Legal Protection of Personal Data of the Republic of Lithuania were established in all shopping centres. Not one supermarket provided notification to the State Data Protection Inspectorate of video surveillance of visitors to the shopping centre. During the three investigations performed in the shopping centres, it was established that, by carrying out video surveillance, the viewing area covered additional territory, exceeding that owned by the centres (i.e. road crossings, dwelling houses, gas stations, cash dispensers, rental premises of other entities, etc.). Excessive personal data was therefore being processed.

In three shopping centres, data subjects were not informed by any means of being monitored by the video surveillance in place. In one shopping centre individuals were informed about the surveillance at the entrances to the centre, but people entered into the monitoring area before being able to read the information (i.e. in the car park). The processing of personal data obtained during video surveillance, the security measures installed and location of video surveillance cameras were not regulated by any documents.

In one shopping centre photographs of shoplifters were found in the vicinity of a video surveillance camera, as well as names, copies of personal identity document, and copies of documents, containing personal information, prepared by the police. Photographs of detained shoplifters and their children were found in the vicinity of another camera. These two shopping centres claimed that this data was needed in order to identify persons and to prevent shoplifting in the centre, that they did not aim to make it public or disseminate it to third persons and that such data was accessible only to security staff. The State Data Protection Inspectorate established that excessive personal data was collected (photos of children that are not related to the prevention of theft; personal identification codes, records of convictions, family status, etc.) for the prevention of theft. Instructions were issued on the violations of the Law on Legal Protection of Personal Data of the Republic of Lithuania to the shopping centres.

Public awareness

1. Events marking the European Data Protection Day organised by the State Data Protection Inspectorate and the Seimas European Information Centre were held on 26 January 2007 at the information centre of the Committee on European Affairs of the Seimas of the Republic of Lithuania: These included the press conference "Personal Data Protection in Lithuania", a conference entitled "Personal Data Protection Problems and Outlook", and discussions with specialists from the State Data Protection Inspectorate. The topical issues of use of biometrical data, video surveillance and data protection in the field of electronic communications were addressed at the press conference and presentations. During the event, the specialists from the inspectorate participated in discussions and provided consultation on personal data protection issues.

2. In 2007, the State Data Protection Inspectorate celebrated its ten-year anniversary. On this occasion on 15 November 2007, the ten-year activities of the State Data Protection Inspectorate were presented to the public institutions of Lithuania, and on 13-14 November 2007 an international conference "Data Protection Tendencies in Information Society" took place. The conference focused public attention on the rapid developments of information technologies, their rapid arrival in Lithuania, positive aspects as well as the ways of preventing the increasing threat to individuals' right to private life due to the processing of personal data. The threat to personal privacy creates greater interest of how to ensure data protection in this sphere. The presentations delivered at the conference dealt with the issues of personal identification in the e-environment and providing e-government services; data retention according to the Directive 2006/24/EC and the implementation of this directive; personal privacy protection in publicising courts' judgments and state institutions decisions; and employees' personal data and video surveillance data processing. At the conference, experiences were shared not only by the mediators from Lithuanian public and private institutions but also by the Data Protection Commissioners and representatives from data protection institutions abroad.

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/EC)

The law of 27 July 2007 modifying some provisions of the law of 2 August 2002 entered into effect on 1 September 2007. The purpose of the new law was to thoroughly simplify some of the old provisions which were held as being an unnecessary administrative burden, without adding any tangible added value to the effective protection of data subjects. The most notable changes concern:

- a vast extension of the conditional "*exemption from notification*" cases in respect of very current data processing situations,
- an extension of the "*exemption from notification*" cases for certain professions,
- simplification of the appointment of a data protection official, function which may henceforth be assumed by an employee of the controller,
- the exclusion of legal persons from the scope of application of the law,
- the modification of some key term definitions (i.e. concepts of consent, personal data, surveillance, etc.),
- the modification of the provisions relating to the processing of special categories of data,
- the introduction of additional grounds for the legitimation of processing for surveillance purposes,
- the case of video surveillance of third parties without any recording of the images, which is henceforth excluded from the mandatory "*prior checking*" (authorisation by the *Commission nationale pour la protection des données*).

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/EC)

The above mentioned law of 27 July 2007 also operates some amendments to the law of 30 May 2005. The objective of the Luxembourg legislator was to clarify some of the provisions of the initial text of law in order to obtain a more accurate translation of the provisions of Directive 2002/58/EC. In addition, the data retention period of traffic data has explicitly been reduced from 12 to 6 months.

Decrees and secondary legislation

The Grand-Ducal Regulation of 12 June 2007 sets out the modalities for establishing the register of legal persons providing services, held by the Luxembourg Chamber of Trade. *Inter alia*, the decree specifies the precise categories of data to be stored in such a register.

The Grand-Ducal Regulation of 1 August 2007 authorises the creation and utilisation by the police of a video surveillance system in public "*security areas*". The regulation provides for many safeguards of data subjects' rights, as, *inter alia*, access to such surveillance is strictly monitored and data retention is limited to 2 months. The administrative regulation dated 27 September 2007 designates explicitly which areas are deemed to be "*security areas*" and in which the video surveillance will be operated.

The Grand-Ducal Regulation dated 21 December 2007 sets forth the amounts and methods of payment of the fee to be collected by the CNPD for any authorisation or any amendment thereof.

Other legislative developments

The government has requested the opinion of the CNPD on the draft law on the administrative and judicial cooperation between public administrations. Within its initial and follow-up recommendations, the CNPD has suggested that the concept of "*data combination*" in the draft did not respect the conditions provided for by the law of 2002, in order to be deemed lawful processing. Hence, the recommendations of the CNPD to the legislator to review the definitions of the draft, to provide for guarantees relating to specific categories of data, to define the different types of inter-administration cooperation and to stipulate guarantees in respect of data confidentiality. Both recommendations issued by the *Commission nationale* have been followed by the Luxembourg government.

The CNPD also advised the government on current topics and affairs like draft law on the cadastral survey of rents, the creation and utilisation of the general information system operated by the police, the draft law

introducing a new allowance for children and the draft Grand-Ducal Regulation determining the 10 databases, held by public legal persons, to which magistrates and police officers will have direct access.

B. Major case law

Civil and criminal case law

District Court of Luxembourg, Court of Appeals, 10th correctional chamber on the validity of proof (video surveillance images) collected in violation of the law of 2002 on data protection

The ruling of the 9th correctional chamber (dated 13 July 2006) determining 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, has been confirmed by the Court of Appeals, 10th correctional chamber on 28 February 2007.

The above ruling of the Court of Appeals has been subsequently brought before the Supreme Court of Appeals ("*Cour de Cassation*"), which rescinded the decision of the Court of Appeals. The Supreme Court quoted Article 6 of the European Convention on Human Rights and, more specifically, the right to a fair trial. After enumerating the different hypotheses under which a judge can discard unlawful evidence from proceedings, it held that a judge has nevertheless the right to determine the admissibility of such unlawfully obtained evidence if he takes into account the elements of the case as a whole, including the method of obtainment and the circumstances under which the unlawful act has been committed. The Supreme Court of Appeals concluded in its ruling that the Court of Appeals refused in a peremptory way to take into consideration all the elements of the case and that it has thereby violated Article 6 of the European Convention on Human Rights. Consequently, the Supreme Court of Appeals rescinded and annulled the ruling and referred the case back to a different composition of the Court of Appeals.

The Court of Appeals (otherwise composed) ruled on 26 February 2008 that the combination of the production of proof obtained illicitly in proceedings (*i.e. without prior authorisation from the CNPD*) and a procedure which itself is not in accordance with the provisions governing the exercise of the criminal prosecution and judicial investigation resulted in a violation of the right to a fair trial.

District Court of Luxembourg, 12th correctional chamber on the breach of Articles 5 and 6 of the law of 2002 on data protection

On 11 October 2007, the District Court of Luxembourg, 12th correctional chamber issued its first penal conviction of an individual on the basis of the law of 2002. A Luxembourg journalist publicly divulged, circulated and sold a list of names of the members of the "*Grande Loge de France*" (a list containing the members of the free-masons in France) through his weekly paper as well as his internet site. The publication of such lists had previously been prohibited by the French "*Commission Nationale de l'Informatique et des Libertés*" (CNIL) in France. The CNIL officially denunciated this offence to the Luxembourg DPA. The *Commission nationale* analysed the case and decided that a breach of the law of 2002 had taken place and therefore filed a complaint with the public prosecutor's office. In its ruling, the District Court of Luxembourg held that the journalist infringed Articles 6 (5) (communication of special categories of data to third parties) and 5(2) (no legitimacy condition provided for by the law corresponded to the data processing carried out by the journalist) of the Data Protection Act of 2002.

Administrative case law

On 21 May 2007 the Administrative Court rejected the request for cancellation of a decision taken by the *Commission nationale*, which authorised the main video surveillance within a big supermarket mall, but rejected the permanent video surveillance of two interview rooms. The *Commission nationale's* argumentation that no legal provision of the law of 2002 authorises the company owning the mall to film and record questioning of alleged shoplifters was upheld by the Administrative Court. The above decision was confirmed on 13 December 2007 by the Administrative Court of Appeals.

C. Major specific issues

During 2007, the CNPD carried out an exhaustive audit of the main Luxembourgish telecommunication operators. The aim pursued by the CNPD was to obtain an overview of how the telecommunication operators made their business compliant with the provisions of the law of 30 May 2005, implementing Directive 2002/58/EC.

In 2007, the *Commission nationale* used its investigative powers granted by the law of 2002 in order to verify the compliance to a decision refusing the authorisation of video surveillance. The results of such investigation showed that the stores did comply with the court's ruling, as no video surveillance was operated in any of the controlled shops.

The CNPD pursued its information and awareness raising campaign, *inter alia*, by actively participating in the first Data Protection Day, organised by the Council of Europe. The *Commission nationale* provided information on the new provisions of the law via its website and through interviews in the Luxembourgish media.

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

None to report.

C. Major specific issues

During the year under review, the Office of the Data Protection Commissioner received 37 complaints with the major topic being the improper use of CCTV cameras. In the course of its investigation, the Office carried out 7 inspections; 3 of which following a complaint and the others as periodic reviews in terms of EU requirements.

During 2007, 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, security, gaming and Police. Consultation meetings were specifically held with the electronic communications sector in connection with the transposition of Directive 2006/24/EC on the retention of data generated and processed in relation to the provision of publicly available electronic communications services. Also, the Office maintained close co-operation with other regulatory authorities, associations and federations.

During the year, the Office gave its contribution to the European and international fora by participating in the Article 29 Data Protection Working Party, the European Conference of Data Protection Authorities, the International Conference on Privacy and Personal Data Protection, meetings of the Joint Supervisory Authorities of Schengen, Customs, Europol and Eurodac, the Case Handling Workshop and the Council of Europe Eurojust and the Bureau of the Consultative Committee of the Convention for the Protection of Individuals on the Automatic Processing of Personal Data.

Presentations were delivered to various organisations and constituted bodies with the objective to further raise awareness and involve the key players in the evolution of the data protection culture. Articles and presentations on different aspects of data protection were published in local media and presented in the radio and television. A substantial number of queries, both by telephone and by e-mail, were handled the Office.

On 28 January, the Data Protection Commissioner joined the other Data Protection authorities in Europe to celebrate Data Protection Day for the first time. This day coincides with the opening for signature of Convention 108 of the Council of Europe, entitled Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which took place in Strasbourg in 1981. This was an occasion for European citizens to be made more aware of their right to privacy in terms of the protection of personal data.

In a resolution issued by the Article 29 Working Party, the forum for the data protection authorities in Europe, for this occasion explained that in a time of omnipresent data processing, this initiative offered an excellent occasion to show and understand how necessary privacy protection should be in a democratic society. Authorities have agreed that, in the future, a more co-operative stance should be taken with the Council of Europe to make this data protection day a success and to show that fundamental rights are best defended by data protection authorities.

To mark the Day, this Office has made a prior announcement through the Department of Information by a Press Release, participated in a local TV education programme and distributed information material, including posters and rulers, to school children. Also, with the assistance of the Office of the Prime Minister, the Commissioner addressed all the Data Protection Officers within the Public Service.

The Netherlands

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

Directive 95/46/EC was transposed into national law, the *Wet bescherming persoonsgegevens* (Wbp) [Dutch Data Protection Act]. This was done by an act of 6 July 2000[8] 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[9]. Other legislation transposing parts of this directive are amongst others the *Wet op de Economische Delicten* (Act on Economic Offences), that implements Article 13(4) of Directive 2002/58/EC.

B. Major case law and major issues

Compliance with the Dutch Data Protection Act is not only in the interest of individual citizens. Respect for individual privacy also serves a collective interest: a society in which we can assume that our personal data will not be misused, making it possible to trust the government, companies, institutions *and* each other.

In 2007, the Dutch Data Protection Authority, *College Bescherming Persoonsgegevens* (CBP), changed its strategic direction and shifted its priority to carrying out investigations and enforcement actions – the core task of any independent supervisory authority – to ensure a more effective promotion of the awareness of standards, and a stronger, more efficient enforcement of the compliance with legislation. Of course, enforcement action must be preceded by clarity concerning the standards underlying our action. In order to be able to achieve this change in course geared towards standards, investigation and enforcement, and given the budget allocated to us, we give priority, as regards requests for help and assistance, to serious violations of a structural nature and to violations which entail major consequences for a substantial number of citizens or for groups of citizens. Through the enrichment and broadening of general information on the Dutch DPA website, citizens are encouraged and helped to resolve their problems themselves and also, where necessary, to take action themselves.

In other words: as a supervisory authority, to exercise the maximum influence possible on compliance with the statutory provisions entrusted to our supervision, we started to intensify general information policy last year, putting citizens, professionals and organisations in a better position to be aware of and comply with (or ensure compliance with) their rights and obligations. We also started to give priority to the tasks falling upon an efficient and effective supervisory authority: investigating how compliance with the relevant statutory provisions is being observed and, when a violation is identified, taking enforcement action.

Large-scale data collection and processing was high on the agenda of the Dutch DPA in 2007, just as it has been in other years. At a national level, privacy problems in relation to the *OV-chipkaart* (digital transport pass) and the *Elektronisch Patiëntendossier* (electronic patient file) are salient issues. These and other subjects will be discussed briefly below in a selection from the activities undertaken in 2007.

Healthcare

The Dutch DPA issued critical advice on a draft legislative proposal that provides for the introduction of an electronic patient file. In the opinion of the Dutch DPA, making patient files available to all care providers is far too risky, partly in view of the protection required for particularly sensitive personal data. With the exception of emergency situations, only care providers with a treatment relationship with a patient ought to have access to the record in question. If this is not the case, there is a risk that unauthorised parties will misuse or misappropriate the medical data.

In 2007, the Dutch DPA also issued negative advice on making the *elektronisch kinddossier jeugdgezondheidzorg* (electronic child record for the youth healthcare sector)

[8] 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.cbpweb.nl.

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

compulsory in the legislative proposal that relates to youth healthcare and infectious diseases. The need for the central electronic storage of data had not been substantiated sufficiently. The Cabinet has since said that it is no longer seeking to create a central electronic child record and that it is looking for other ways to exchange communications in the youth healthcare sector.

Public administration

The BSN [citizens' service number] was introduced at the end of November 2007. This marks the start of a new phase for the Dutch DPA. At the BSN management facility, a personal public service point will be created, which local authorities and citizens can approach with any questions they may have. As the authority responsible for supervision of the careful handling of personal data, the Dutch DPA is the authority with competence to intervene in the event of real problems with implementation of the act.

The Dutch DPA also expressed its criticism of the proposal for a *verwijsindex risicojongeren* (VIR) (national reference index of young people at risk). The Dutch DPA agrees wholeheartedly with efforts to achieve better and faster help for children and young people with problems, but it is not yet clear whether the sole objective of the reference index is the provision of assistance, or whether its aim is also to help maintain public order. It is important for there to be complete clarity about key terms and criteria.

Police and the judicial authorities

Safety and privacy are both vital for citizens. However, all too often in public debate, these values are, rather simplistically, construed as opposing values. To help put the discussion back on course, the Dutch DPA, in collaboration with the Ministry of Justice and the Ministry of the Interior and Kingdom Relations, commissioned research into the identification of the most appropriate balance between the efforts to achieve a safe society and the efforts to safeguard the right to privacy. The resulting external research report, with guidelines for more effective dialogue, was presented at a symposium on 1 November 2007.

In situations where the police tap telephone calls in the context of criminal investigations, conversations between lawyers and their clients are often recorded too. These conversations with holders of confidential information entitled to privilege must be erased as soon as possible. A Dutch DPA investigation of the national wiretapping rooms shows that this does not happen correctly or on time in far from all cases. The Public Prosecution Service has announced that measures for the improvement of this situation will be implemented.

In recommendations on proposed new legislation, or other regulations in the field of criminal law, the Dutch DPA regularly raises the following question: has it been demonstrated that the regulations in question are really necessary? Is it clear that existing or previously proposed statutory possibilities fall short? For example, in the opinion of the Dutch DPA, in the light of improved identification possibilities in the future, the Minister of Justice has provided insufficient justification for the proposal for a central database for the storage of the identity of all suspects and convicted offenders. And do the plans by the police, the Public Prosecutions Department and the *Koninklijke Marechaussee* (KMar) [Royal Netherlands Military Constabulary] to record the registration number of all motorists entering Amsterdam via the *Utrechtse brug*, regardless of whether they have a clean record or not, really contribute to a safer society?

At the end of 2007, at the request of the Senate, the Dutch DPA issued advice on a legislative proposal that would extend the powers that the intelligence and security services, in their efforts to combat terrorism, have to obtain data on travelling, payment traffic and Internet use by citizens. The Dutch DPA believes that the need for these measures, in addition to the many measures already in existence, has not been demonstrated and considers that the consequences of this data analysis for individual citizens, but also for responsible parties and the services involved, have not (or not sufficiently) been recognised.

Trade and services

Following the announcement by the Dutch DPA that it would take enforcement action against the unlawful combined storage of the name and address details of travellers and their travel data, the public transport companies would seem to have finally recognised that the *OV-chipkaart* has consequences that are contrary to the

Wbp. In 2007, in a pilot on the Amsterdam metro network, research was done into the impact of the card, which concluded that the *OV-chipkaart* system is being used unlawfully. The *Gemeentevervoerbedrijf* (GVB) [Municipal Transport Authority] and other public transport companies have now undertaken to bring practice into line with the Wbp. In the technical design for data storage, a distinction will be made between name and address details, on the one hand, and travel movements on the other. As a result, the risk of the unlawful monitoring of individuals' travel behaviour will be limited considerably.

The Internet

Personal data is published on the Internet in many different ways and is generally accessible worldwide, 24 hours a day, to an extensive and diverse public. There can be unexpectedly serious consequences for Internet users – many of whom are children – whose personal data is on the web. In 2007, the Dutch DPA developed and published guidelines in order to clarify what is permitted and what is not when publishing personal data on the Internet. The individuals responsible can use these guidelines to assess whether publication of personal data on the Internet is permitted. A large amount of information material has also been published on the Dutch DPA site. As regards minors, the Dutch DPA takes a proactive stance in providing the rules applicable for social networks and for online marketing.

The government also makes use of the Internet. In 2007, the Dutch DPA conducted an investigation into how the municipality of Nijmegen publishes data on planning permission. Complete scanned copies of application forms were published on the net, containing not only data on the property in question and on the alterations proposed, but also personal data on the applicant, including his/her signature. In the opinion of the Dutch DPA, the municipality may only publish compulsory data on the Internet – on the property in question and the alterations proposed.

The proper performance of a public-law task does not justify a situation where an administrative body automatically publishes all data on the Internet. The Dutch DPA will also publish guidelines on the privacy aspects of active public disclosure in the framework of the Wet openbaarheid van bestuur (Wob) [Government Information (Public Access) Act] in 2008.

Work and social security

Citizens do not automatically become suspects simply because they receive benefit or housing benefit. In the Waterproof project, old-age pensioners and recipients of a social assistance benefit in 65 municipalities in Friesland, Groningen and Drenthe were checked for fraud based on data concerning their water consumption and the water contamination surcharge. The data obtained was also used to check fraud with housing benefit. The Dutch DPA investigated this linking of computer files and ruled it unlawful. It is important to combat benefit fraud, but monitoring based on the linking of computer files is only permitted on the basis of sound risk analysis, since this makes it possible to show that it is necessary to further monitor a group of citizens at a high risk of entering the fraud zone. As a result of the Dutch DPA ruling, the *Sociale Inlichtingen en Opsporingsdienst* (SIOD) [Social Security and Investigation Service] is now working on the development of risk analyses using Privacy Enhancing Technology (PET). In this way, combating fraud and the protection of personal data seem to go hand in hand.

Another way of uncovering benefit fraud is covert observation by social security investigators. The processing method used for the personal data connected with these activities has been laid down in a process description approved by the Dutch DPA. Research in 2006 showed that compliance with the obligation to inform citizens of the fact that they had been observed left something to be desired. The process description was then tightened up in 2007.

In the event of a transition to an occupational health and safety service provider, can the old service provider transfer employees' records to the new service provider without this being provided for by law? The Dutch DPA ruled 'no' in 2006. Further to indications from the field that this view caused problems, the Dutch DPA did research in 2007 to ascertain whether a different approach is possible within the existing statutory frameworks. This led to an outcome whereby transfers were made subject to a distinction between data that is not subject to medical professional secrecy and data that is. In the first case, the data may be transferred. In the second case, data may only be transferred under certain conditions.

Poland

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

Telecommunications Law
In the reporting period, work was carried out on the amendments of the Act of 16 July 2004 – Telecommunications Law that implements into the Polish legal system the provisions of the Directive 2006/24/EC of the European Parliament and of the Council 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. A proposal was made to extend the storage period of transmission data concerning subscribers and end users which may be disclosed to authorised bodies responsible for national defence and security and public safety from 2 to 5 years. It was argued that the extension of the above mentioned period would increase the effectiveness of actions carried out by the law enforcement authorities in the course of criminal proceedings and investigations taking into account that billing information and other telecommunications data are very strong evidence. Finally, the draft amendments of the Telecommunications Law have not been adopted.

Banking law
In 2007, the amendment of the Act of 29 August 1997 Banking Law (unified text: Journal of Laws of 2002 No 72, item 665) entered into force. Among other provisions, Article 105 a of the above mentioned Act has been amended. The legislator introduced the possibility for banks and other institutions authorised to grant credit may process data on natural persons covered by banking secrecy, after the expiration of the obligation under a contract concluded with a bank or other institution authorised by the act to grant credit without consent of the data subject for statistical purposes for the period of 12 years after the expiration of the obligation. So far, banks and the above mentioned institutions may process data on natural persons covered by banking secrecy for no longer than 5 years from the expiration of the obligation.

Schengen Area
On 24 August 2007, the Act on the participation of the Republic of Poland in the Schengen Information System and the System of Visa Information that implements *the Schengen Acquis* was adopted. It determines, *inter alia*, the obligations of authorities authorised to issue alerts and make access to data contained in the Schengen Information System and Visa Information System via the National Information System. Poland entered the Schengen Area on 21 December 2007.

Cooperative law
The provision ordering the disclosure of housing cooperatives' documentation including personal data (by posting information on the Internet) was introduced under the Act of 14 June 2007 on the amendment of the act on housing cooperatives and other acts. Such documentation may be disclosed to persons who are neither a member of the housing cooperative concerned nor in charge of the cooperative's activities. From the moment of publication of such information, on-line personal data (sometimes also sensitive data) may be obtained and used by third parties.

Social Welfare
The Act of 16 September 2007 on assistance for persons entitled to maintenance does not determine any guidelines that should be taken into account by the Minister for Social Welfare while preparing secondary legislation as to the scope of data which is to be collected in the Maintenance Debtors Central Registry. Despite the resolute reservations submitted by the Inspector General for Personal Data Protection, they were not taken into account during legislative work on the draft of the above mentioned act. As a result, a draft regulation by the Minister of Labour and Social Policy concerning the scope of data collected in the Maintenance Debtors Central Registry provides for a particularly broad catalogue of data, including sensitive data to be collected there.

B. Major case law

Pre-paid mobile phones' numbers central database
The Inspector General for Personal Data Protection took part in the discussion on the proposal to create a central database of any subscribers and registered users of pre-paid mobile phones operated by the President of the Office of Electronic Communications. The authors

of the proposal stressed that such a database would be essential for emergency services to receive necessary information about a caller and his/her location. The Inspector General indicated that such information could also be obtained according to the procedure provided for by Article 78 of the Telecommunications Law. Under that provision, operators of public telephone network shall make available information on the location of the network termination point from which the connection to the '112' emergency number and other emergency numbers originates on each and every request made by emergency services called upon by the law to provide assistance, allowing for immediate intervention.

Social networking website 'Nasza-klasa' – inspected.
The Inspector General for Personal Data Protection inspected social networking website 'Nasza-klasa' (where more than 6 million users created their profiles) with regard to the compliance with the requirements of the Data Protection Act. The results of detailed inspection showed that the portal met practically all requirements provided for by the Data Protection Act (introduction of additional security measures was recommended while logging in to the portal) and processes personal data according to its own privacy policy. The portal's owners, who had earlier notified their data filing systems for registration, announced that they would improve their data processing operations according to all of the Inspector General's remarks and recommendations issued after the inspection concerned.

C. Major specific issues

Data Protection Day
28 January 2007 saw the first celebration of the Data Protection Day, established on the initiative of the Council of Europe. It featured many events, in which the Inspector General actively participated. Among the most important ones was the Conference "Personal data protection – a guarantee or a threat to privacy?" organised by the Inspector General for Personal Data Protection, Mr. Michał Serzycki and by the Chancellor of the Kozminski Business School in Warsaw, under the patronage of the Marshall of the Sejm, honoured by the presence of numerous representatives of scientific circles specialising in personal data protection, as well as members of Parliament and representatives of government authorities. The Inspector General for Personal Data Protection announced a number of educational initiatives aimed at increasing public awareness in the field of personal data protection and the right to privacy and hence at increasing the protection of personal data in Poland. On 31 January, celebrations took place at the premises of the Permanent Representation of Poland to the European Union in Brussels. Many people concerned with the problems of data and privacy protection in the European Union institutions, the Council of Europe, as well as Polish members of the European Parliament, representatives of the Polish diplomatic agencies in Belgium and Polish and foreign journalists were invited to this occasion.

The Inspector General also gave a number of interviews to the press and various television channels.

Educational campaign
In 2007, the Inspector General launched a wide-ranging educational campaign aimed at increasing social awareness in the field of data protection. The educational actions comprised drawing competitions for children entitled "Privacy around me" and a competition for the best MA thesis on data protection. Furthermore, the Inspector General signed an agreement with one of Warsaw's business schools concerning the creation of postgraduate studies in data protection.

The employees of the Bureau of the Inspector General for Personal Data Protection carried out a number of workshops for the employees of other institutions, including major government authorities such as the Chancellery of Sejm and Senat, the Ministry of Foreign Affairs, the Customs Office and the National Bank of Poland. They also participated actively in the events organised by other entities. In order to bring the data protection issues closer to the general public, they also took part in the Customs Service Conference in Olsztyn and in the scientific conference "10 years of the Polish Data Protection Act" organised by the University of Torun. A number of educational meetings with the students of various Polish universities were also carried out.

The Bureau of the Inspector General for Personal Data Protection also cooperates with the Polish Members

of the European Parliament, organising workshops on personal data protection. The framework of educational actions planned for the year 2007 also comprises the conference "Right to Privacy in Surveillance Society" which is to take place in Warsaw on 22 and 23 October.

Conference – right to privacy in surveillance society

The conference commemorating the 10th anniversary of the adoption of the Polish Data Protection Act took place on 22 and 23 October 2007 in the Column Room of the Sejm (Polish Parliament).

It was accompanied by workshops entitled "Privacy and the Media" organised in cooperation with the European Commission, which allowed the discussion of questions of privacy and data protection in the context of journalism.

Many distinguished speakers, both domestic and foreign, presented the most important issues concerning the protection of personal data and privacy to the participants of the conference.

The aim of the conference was to discuss the important aspects of the Data Protection Act which are particularly important now in the age of rapid development of new technologies, especially information technologies.

The three sessions planned for 22 October 2007 featured such issues as new technologies – new possibilities of surveillance, European Information Systems and the role of Data Protection Commissioners in surveillance society. The first session concentrated on different aspects concerning new technologies and the possibilities of surveillance that they create. The second session concerned the European Information Systems. The ever more important role of Data Protection Commissioners, who protect the right to personal data and privacy protection in the European countries, was the subject of the third session.

On the second day of the conference, the "Privacy and Media" workshops allowed the discussion of current issues concerning privacy and data protection in the context of journalistic activities and the chairs of respective sessions – representatives of the European Commission and the European Data Protection Authorities – gave the participants an opportunity to reflect on protecting the privacy of public persons and Internet users.

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 Law.

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.

No further legal dispositions were approved directly concerning the implementation of the above mentioned directives. However, several acts entered into force involving data protection matters, such as Law 7/2007, regulating a new ID card for all citizens above six years of age. This card contains the civil identification number, the tax identification number, the social security number and the health card number. It also contains a fingerprint and a digital photograph. The new citizen card – as it is designated – allows both physical and electronic identification. It raised a lot of major issues on data protection, which the DPA expressed in its opinions during 2006.

Law 33/2007 regarding video surveillance in taxis has also entered into force, providing the possibility for taxi drivers to install video cameras in their vehicles. The system foresees that the taxi driver only switches on the camera whenever he feels in danger. In that case, the images are transmitted to a private central unit – to which the taxi is connected - where they are recorded and eventually communicated to law enforcement authorities for investigation, in case of any eventual security problem; otherwise, the images are deleted.

The law states that the central units are the data controller and they must provide notification of this data processing to the DPA, which also supervises the security measures installed and the reliability of the equipment used.

B. Major case law

During 2007, there was an important decision from a Central Administrative Court as the result of an appeal against a DPA decision concerning the use of video surveillance in a condominium. The decision was favourable to the DPA.

Within its competences to authorise the use of video surveillance for the purpose of protecting people and assets, the DPA only authorises the installation of such systems inside condominiums if residents and owners unanimously consent. In this case, the DPA authorised the use of video surveillance systems, assuming that this unanimity had been achieved, after receiving information from the data controller. However, it turned out that the consent of all residents had not been obtained, and the DPA revoked the authorisation, which was given on a false basis. The data controller challenged this last decision, arguing that it was excessive of the DPA to demand unanimity as a condition for the authorisation, and that the authorisation could not be revoked. The court decided that the authorisation decision could be altered (as it was based on inaccurate facts) and that it was quite pertinent and proportional to make the use of such systems in condominiums subject to the residents' unanimity, considering the intrusion into private life that video surveillance represents.

C. Major specific issues

Opinions to draft laws

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

In 2007, the DPA provided 62 opinions, some of them related to bilateral agreements between Portugal and third countries, in the area of police cooperation, and also regarding several other issues containing data protection dispositions, in particular: development of e-government measures (simplification of procedures, replacement of hard copies by digital documents, online accesses, data interconnections), regulation of the National Statistics System, central database on life insurance beneficiaries, hotel forms for foreigners, credit risk assessment central database.

The DPA also gave an opinion on the transposition of Directive 2006/24/EC on traffic data retention, suggesting important amendments, especially concerning the need

to clearly state the purpose, to define "serious crimes" under national law, and to shorten the data retention period, which according to the proposal was 2 years. Indeed, the DPA opinion was mostly taken into account and the retention period was set at 12 months.

In 2007, the DPA gave two relevant opinions on the establishment of DNA databases for criminal investigation purposes and for civil identification purposes, the latter being on a voluntary basis. The DPA raised a lot of concerns related to this proposal. Some suggestions were implemented in a new draft, but one of the most significant matters – the DNA database for civil identification purposes – was adopted anyway.

Guidelines for clinical studies
In 2007, the Portuguese DPA issued important guidelines for data controllers regarding data processing for the purpose of conducting studies in the health sector and also for the purpose of clinical trials on experimental medicines for human use. These guidelines allowed a faster authorisation procedure and set out the requirements that should be met by data controllers. At the same time, data subjects become aware of the framework conditions for the processing of their data and their rights.

Video surveillance in public areas
The Portuguese DPA gave its first opinion concerning the use of video surveillance systems in the streets. This possibility results from Law 1/2005, which regulates the use of video surveillance by law enforcement authorities. According to this law, the municipalities can also request the installation of such systems in the streets, after a positive opinion from the local police. In case a negative position is given, the DPA then issues an opinion, which becomes binding. In the event of a positive opinion from the DPA, the final decision rests with the Ministry of Internal Affairs.

Therefore, the municipality of the city of Porto requested authorisation to install video cameras in some city centre streets for security reasons in a very crowded area of restaurants, bars and esplanades. The system foresaw the use of blank zones for the residential buildings with all the images being transmitted directly to a police station. The DPA gave a positive opinion, except for the use of the system during the day when it has to be switched off (as the criminality problem was mainly at night) and for sound recording, which the DPA considered disproportional and quite intrusive, in particular in such a leisure area where conversations from people outside on the esplanades could be heard and recorded.

The Ministry of Internal Affairs therefore provided the final authorisation for the use of the video surveillance system, but within the conditions set by the DPA. According to the law, this authorisation is valid only for one year, after which its continuity has to be evaluated by analysing whether the conditions that led to the installation of the system are still pertinent, as well as whether the purpose (criminal prevention and prosecution) has been achieved.

Protocol with the Ministry of Education
In the celebration of the first European Data Protection Day, the Portuguese DPA signed a protocol with the Ministry of Education to include curricular plans, at all teaching levels (1-12), covering data protection matters in the public schools.

This protocol is of major importance as it will allow the long-term and systematic introduction of a data protection programme into the educational system of schools. The aims are to contribute to raising awareness of data protection issues, to promote correct use of new technologies and to develop and strengthen a privacy culture among the youngest, helping them to fully achieve, as citizens, their informational self-determination.

Through this protocol, the Ministry of Education is promoting the dynamics for the adoption of this pedagogic project in the schools network. The DPA produces all relevant materials addressed to the pupils to be distributed in schools with the support of the ministry.

Following the signature of this protocol, the DPA distributed a poster about the Internet for children aged between 10 and 15 and, in a first phase, started working on a specific structural program for children of those ages, which was presented to the ministry in October 2007. This project was launched in January 2008 in the schools.

Data Protection Essay Prize
Last year, the DPA launched a Data Protection Essay Prize to be awarded annually to any work developed on data protection, either from a legal, sociological or technical perspective.

The aim is to encourage the analysis, the reflection and the production of original work in the field of data protection. The prize is the publication of the winner's work. The official prize presentation ceremony takes place every year on 28 January as part of the celebration of the European Data Protection Day.

In this first year, the prize was awarded and an honourable mention made in December 2007.

V Iberian-American Meeting on Data Protection
In November, the Portuguese DPA hosted the V Iberian-American Meeting on Data Protection in Lisbon with the participation, as observers, of African Portuguese-speaking countries. The meeting approved Directives for the Harmonisation of Data Protection in the Iberian-American Community, as well as the Lisbon Declaration, which highlights the recent developments in some countries for the adoption of data protection legislation, and stresses the importance in a globalised economy of promoting easier mechanisms for international data transborder flows safeguarding the fundamental right to data protection.

The Iberian-American Meeting underlined too the incentive given to this community to sign the Convention 108.

Romania

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

The provisions of Directive 95/46/EC of the European Parliament and Council were transposed into Romanian legislation on 12 December 2001 by the adoption of Law No 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

Law No 677/2001 has granted full independence to the supervisory authority and has invested it with powers of investigation, control and intervention, consultation, regulation and public information, by taking over the principles established by Directive 95/46/EC.

The Supervisory Authority's powers were initially entrusted to the Office of People's Advocate (Ombudsman). However, following the European Commission's request to establish an independent, autonomous supervisory authority that could carry out specific monitoring and control attributions in the field of personal data protection as provided by Directive 95/46/EC, the Romanian Parliament adopted Law No 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing, published in the Official Journal of Romania No 391 of 9 May 2005. According to this law, the National Supervisory Authority for Personal Data Processing is a public authority with legal personality, autonomous and independent in relation to any other public authority, as well as to any other natural or legal person of public and private law.

An important modification introduced by Law No 102/2005 to the provisions of Law No 677/2001 consisted of abolishing Article 27 paragraph (5) of the latter, according to which the Supervisory Authority had to obtain the consent of the prosecution authority or competent judicial court before starting an investigation concerning personal data processing carried out in the field of criminal law.

Another modification was made to Law No 677/2001 by Law No 278/2007 which abolished the notification fee for personal data processing which falls under the scope of Law No 677/2001.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector has been transposed into national legislation by Law No 506/2004 on the processing of personal data and the protection of private life within the electronic communications' sector.

Law No 506/2004 guarantees the protection of personal data processed by the public electronic communication network and service providers, as well as providers of subscribers' registers. This law completes and specifies the legal framework established by Law 677/2001 on the specific requirements of the electronic communications' sector.

Bearing in mind that certain data processing is frequently carried out in the interests of the law or of the data subject and are not liable to infringe the data subject's rights, the President of the Supervisory Authority issued two decisions (Decision No 90/2006 and Decision No 100/2007), published in the Official Journal of Romania, which establish the cases in which the notification of personal data processing is not required.

The Supervisory Authority is consulted whenever legislative acts are drafted and these refer to the protection of individuals' rights and liberties with regard to the processing of personal data, in accordance with the provisions of Law No 677/2001, as modified and amended. This is why the Supervisory Authority has given its notice on several legislative acts, including: the draft decision of the Romanian Government on approving the methodological norms of unitary enforcement of the legal provisions on the evidence, residence, and identification documents of Romanian citizens; the draft decision of the Romanian Government on form and content of identity documents, of the self-adhesive tag on establishing a new residence and buildings' records; the draft law on the obligation of air carriers to communicate passenger data; the draft legislative act of the Romanian Government on the free movement on Romanian territory of EU and EEA citizens and establishing the form and content of the identity documents issued to EU citizens and their family members; the draft law on establishing and organising the National System on Genetic Data.

The Supervisory Authority has also issued several notices on codes of conduct of various professional associations, including the Romanian Brokers' Association, the Romanian Association of Private Practice Stomatologists and the Romanian Banks' Association, which comprise adequate norms on the protection of individuals whose personal data are processed.

Taking into consideration the necessity of ensuring efficient protection for the rights of the individuals whose personal data is processed within credit bureau type systems, and especially in view of the risks this type of automated processing poses to the intimacy, family and private life of the individual due to the nature of the processed data and the processing's purpose, the President of the Supervisory Authority issued in 2007 Decision No 105/2007 on the processing of personal data within credit bureau type filling systems.

This decision establishes the categories of participants to this type of filling systems, the data which may be processed therein and the conditions under which this data may be transmitted, the storage period, the participants' obligations, including ensuring the confidentiality and security of the personal data contained within these systems.

B. Major case law

It was noticed that in 2007 the judicial courts adopted a unitary practice in the cases referring to personal data protection, even though, initially, there were somewhat different approaches at the level of lower courts.

1. Following an investigation carried out at the General Inspectorate of the Romanian Police, the Supervisory Authority was able to ascertain a contravention, notably the failure to notify the processing of personal data by installing surveillance cameras on one of the main national roads, which allowed the identification of the vehicles' registration plates. The fine imposed by the Supervisory Authority was challenged by the General Inspectorate of the Romanian Police in a court of law. This case reached the Romanian Supreme Court. In the end, the High Court of Cassation and Justice supported the Supervisory Authority's decision.

2. Another case in which a court of law issued a ruling was that of the Supervisory Authority fining a kindergarten for processing personal data without any notification to the Authority. The personal data was processed within an operational video surveillance system which captured images of all the children in the kindergarten. In view of the fact that the personal data of both children and staff were processed in this manner without any prior notification to the Supervisory Authority, the Court ruled in favour of maintaining the Supervisory Authority's sanctioning decision as these facts constituted a minor offence (failure to notify).

3. Another case from 2007 concerned a travel agency which automatically filed the e-mail addresses of its customers and was also fined by the Supervisory Authority for failure to notify this type of processing. The Authority's decision was considered to be lawful and well founded by the Supreme Court which thus supported the fine imposed by the Authority.

4. A special case found its starting point in the compliant submitted by an individual who stated that he had received unsolicited electronic commercial messages (spam) from a private company, which infringed the provisions of Law No 506/2004 on the processing of personal data and the protection of private life within the electronic communications' sector. Through it, the lawmaker prohibited the communication of commercial messages through automated systems which do not require any intervention from a human operator, via fax, e-mail or any other method which implies publicly available electronic communication services, except for the cases in which the data subject has clearly expressed his consent. It is also provided that the communication of commercial messages through electronic mail will be prohibited in all cases if the identity of the sender (or on whose behalf the messages are sent) is concealed or if there is no mention as to where the data subject might ask for such messages to be stopped.

As regards the activities of advertising and marketing, the investigation revealed that the messages in fact contained an "opt out" command. Even though the complainant had used this option, commercial messages continued to be sent to his address. As a result, the data controller was sanctioned for infringing the

legal provisions on unsolicited commercial messages and, in this way, he also infringed the right to private life of his customers. This case is still due to be considered before a court of law.

Despite the diversity of issues challenged before the courts, the legal framework on personal data protection has been interpreted by the courts in a similar way to that of the Supervisory Authority.

C. Major specific issues

The Supervisory Authority paid special attention to the correct implementation of the legal framework on personal data protection which meant that the control activities played an important part in the Authority's activity in 2007. 280 investigations were carried out in 2007, 235 of which were *ex officio* and 45 as result of complaints (21) or notices (24) received from the general public.

The majority of the *ex officio* investigations followed the authority's annual plan on specific issues selected from its previous experiences, which indicated poor knowledge of the provisions of Law No 677/2001, a reduced number of notifications submitted by data controllers form various fields and a potential risk to the rights and liberties of individuals posed by these processing operations. The four major fields for each quarter were:

1. **telemarketing** – personal data processing by supplying commercial information services;
2. **debt recovery** – processing the personal data of debtors in order to retrieve debts;
3. **selection and distribution of the workforce** – processing the personal data of applicants for jobs domestically or abroad**;**
4. **tourism agencies** – personal data processing whilst making reservations or providing other services for tourists.

Following the investigations carried out in accordance with this annual plan, a significant increase in the number of notifications was recorded as compared with previous periods. They also led to a better observation of the fundamental rights and liberties of the individuals, especially with regard to the protection of their personal data and their privacy.

Aside from the investigations carried out in accordance with the annual plan, during 2007 a number of investigations were also carried out as a result of the collaboration with other European authorities within the Working Group Article 29, amongst which we can mention the processing of personal data within the SWIFT international financial transaction system.

A significant number of the notifications submitted every year to the Supervisory Authority refer to the activities of marketing and advertising.

As regards the **direct marketing** operations, the Supervisory Authority continued the actions started in 2006 at the level of the Romanian Direct Marketing Association in order to implement the measures required in order to ensure the individuals' right of opposition to receiving advertising material.

A specific form of direct marketing which seems to have been used more and more often recently is that of **telemarketing**. During the course of 2007, ten investigations were carried out in order to check the conditions under which the personal data are processed within this type of activity and sanctions were applied where infringements of the relevant legal provisions were noticed. As a result of these investigations, the following facts were highlighted:

- Generally, the largest companies in Romania carry out this type of activity through their own respective departments ("*inbound*"), or through specialised companies (on a contractual basis). The investigations revealed that data controllers in this field generally notified their processing operations through other companies, specialised in telemarketing services. In some cases, in which the obligation to notify had not been observed, the data controllers were sanctioned in accordance with Article 31 of Law No 677/2001.

The investigations carried out at companies specialised in debt retrieval revealed that personal data of debtors are kept even after the debts were paid. This is why the supervisory authority ordered the deletion of the data which was no longer required to fulfil the specific purpose of the processing (debt collection/retrieval). In other situations, it was ascertained that data controllers

continued to keep debtors' data in order to set up "black lists" which were, in some cases, even published on the internet, on the data controller's website. In these cases, as the principles on the legitimacy and non-excessive processing were not observed, the Supervisory Authority stopped these processing operations and ordered the deletion of the data held and published up to the time of the investigation. Other obligations of data controllers in this field to which special attention was given during these investigations referred to the period for which the data are stored and the adoption of written security procedures.

46 investigations were carried out in 2007 at data controllers which carry out activities in the field of selecting and distributing workers, in order to verify the way in which the provisions of Law No 677/2001 are observed. Following these investigations, the data controllers complied with the recommendations made by the Supervisory Authority. The most frequent infringements in this field referred to failure of the data controllers to properly inform the data subjects and to observe the minimum requirements on the confidentiality and security of the processed data.

In the field of tourism agencies, 35 investigations were carried out in 2007 as a result of which the following infringements of the provisions on personal data protection were ascertained:

- there were few situations in which notifications were submitted by tourism agencies;
- the data subjects were not correctly informed of their rights;
- no notifications were submitted in this field for the transfer abroad of personal data and, as a result of all of these infringements, the data controllers were sanctioned.

Another important specific issue in 2007 was the involvement of the Supervisory Authority in the academic field as part of its campaign to increase public awareness with regard to the specific issues related to the field of the protection of personal data. As a result of the events organised in celebration of the 2007 European Data Protection Day the "Simion Bărnuțiu" Law School in Sibiu and the Supervisory Authority have signed a collaboration protocol. As a result of this collaboration a new field of "personal data protection" has been introduced within the postgraduate courses; these lectures are held by the President of the Supervisory Authority.

Following numerous meetings between members of the academic institution and the President of the Supervisory Authority, an increased interest was noticed amongst students in the field of privacy and personal data protection. As a result of this, careful consideration is being given to the introduction of courses on the protection of personal data and police activities. Negotiations are also being held in order to include a course on "personal data protection" at the private University of Hyperion.

Slovakia

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

Implementation of Directive 95/46/EC

The Office for Personal Data Protection of the Slovak Republic on the basis of its own initiative aimed to achieve a best possible harmonisation of Act No 428/2002 Coll. on Protection of Personal Data as amended by latter provisions (hereinafter referred as to the "act on personal data protection") with the Directive 95/46/EC, has consulted with the Directorate-General for Justice, Freedom and Security of the European Commission. In January 2007, the European Commission stated, on the basis of these consultations, that, with regard to personal data protection, the situation in the Slovak Republic is satisfactory. Nevertheless, in 2008 the Act on Personal Data Protection will be amended in respect of the latest legal and technological developments within the European Union and experience with personal data protection law enforcement.

Other legislative developments

The Office provided its comments to 223 drafts acts, regulations and ordinances of the Government of the Slovak Republic. The most frequent drafts were proposals of the Ministry of the Interior, the Ministry of Health and the Ministry of Agriculture of the Slovak Republic. This means a substantial increase, not only in numbers, but also in the general awareness of the state administration bodies involved in the national legislation process, particularly of their need to cooperate with the national personal data protection Supervisory Authority more closely.

By the end of 2007, Directive 2006/24/EC (Data Retention Directive) had been implemented into Slovak law as the amendment of the Act on Electronic Communications. The retention period concerning operational data, localization data and data on communicating parties has been set at 6 months with regard to Internet communication data and at 12 months for other types of communication.

Within the legislative activities relating to the preparation for Schengen accession, partial amendments of a special act and a governmental decree were provided and adopted, namely the amendment of the Act of Police Corps and of a Decree of the Ministry of the Interior. The office's proposal to designate the Ministry of the Interior as the controller of the Schengen Information System as well as the controller of all other police information systems has been accepted. With the passing of this act, a final step for the successful inclusion of the Slovak Republic to the Schengen Area has been conducted.

B. Major case law

In 2007, two cases resumed from the past years – in one of them the Ministry of Justice of the Slovak Republic sued the Office for its decision from 2006 on unlawful publication of the national identification number (so-called birth number) on the internet pages of the Commercial Bulletin. The Office, in accordance with the diction of the Act on Personal Data Protection, ordered that all published birth numbers should be removed from the web or made unreadable. The Ministry submitted an objection against the order and asked the Office to nullify it. The Office refused the objection of the Ministry. The Ministry used its right for judicial protection and submitted the case to the regional court. The court fully denied the claim of the Ministry and confirmed the order of the Office at the end of January 2008.

In the latter case, a data subject sued the Office for not issuing a legal measure against a newspaper publishing company that enabled the publishing of personal data of a data subject on its website without his knowledge. At the same time, the website enabled anyone to publish various opinions. The petitioner claimed that an unknown person put his personal data, including his name, surname and address, on the website. The petitioner asked the regional court to decide that his rights, stipulated in the Personal Data Protection Act, were violated while it was known that the said data subject had himself previously repeatedly published his personal data on other sites. In November 2004, the regional court resolved that the procedure of the Office was in line with the Act on Personal Data Protection. The petitioner appealed against the judgement. In May 2007, the Supreme Court fully confirmed the verdict of the regional court, also stating the Office was justified.

C. Major specific issues

In 2007, data subjects and other natural persons filed 121 notifications to the Office alleging that their rights stipulated by the Data Protection Act had been directly infringed upon. 27 notifications were filed by other subjects who alleged suspicion of violation of the Data Protection Act. The chief inspector of the Office ordered 125 proceedings to be conducted *ex officio*. In total, the Office dealt with 290 notifications in 2007. This rather high number also consisted of cases unresolved from the end of 2006.

It is worthy of mention that in 2007 the inspection department conducted a total of 102 inspections of controllers and processors of information systems and made 62 "submissions for explanation". In comparison to 2006, this represented an increase of 65%. In 2007, 104 binding orders have been issued. The Office controlled existing camera systems, particularly those of the city police.

In 2007, the Office imposed seven fines, whereby the sanctions fell in the lower range of the fine scale.

With regard to the preparations for the Schengen accession and following the provisions of the Act on Personal Data Protection obliging controllers to give data subjects detailed information on the processing by gathering their personal data, the Office conducted an inspection in the diplomatic representation bodies of the SR and their consular departments in Serbia (Beograd), Croatia (Zagreb), Ukraine (Uzhorod), Belarus (Minsk), the Russian Federation (St. Petersburg) and Turkey (Ankara, Istanbul). The inspections were also performed in the Office of Border and Foreign Police of the Slovak Republic, Office for Criminalistics and Expertise – Department of EURODAC and on the Customs Directorate of the Slovak Republic.

Swift cause

The European Commission Directorate-General for Justice, Freedom and Security Data Protection Unit asked, in its e-mail dated 20 April 2007, the Office for cooperation in the investigation of the SWIFT case. Among other things it asked for the official opinion of the Office on the present status of measures taken by banks in respect of the legal obligation to inform their clients (data subjects) about the processing of their personal data that were collected for the purpose of bank payments carried out via SWIFT.

In that respect, the Chief Inspector of the Office appealed by letter to 24 banking institutions to carry out complex revision of their duties relating to transborder payment systems performed via Swift in the framework of supervision performance under Section 19, paragraph 4 of the Act No 428/2002 Coll., focused on evaluation whether processing of personal data causes any violation of rights and freedoms of the respective clients (data subjects) or not.

The National Bank of Slovakia was also addressed. While collecting, processing and subsequently transferring the personal data across borders, each bank is obliged to sufficiently inform the respective data subjects about the conditions of their personal data processing (Section 10, paragraphs 1 to 3 of the Act 428/2002 Coll. and Article 10 and 11 of the 95/46/EC Directive). The Office asked the banking institutions to provide their complex and complete position on their particular measures and mechanisms that had been or would be executed to comply with the duties stipulated in points 5 and 6 of Position No 10 on data processing of SWIFT focussing on points 5.3.2., 5.5., 6.1., 6.2., 6.5. and 6.6. If a banking institution did not take the respective measures it was obliged to specify which mechanisms and particular measures will be executed as the personal data processor by 31 May 2007 at the latest. Using these findings, the Section of Inspection of the Office formulated the information for the European Commission that was sent by the President of the Office to the EC on 14 May 2007. By the end of August 2007, the questionnaire concerning fulfilment of the obligation to inform respective bank clients about international payment transfers performed by SWIFT was sent to the EC.

The processing of personal data of clients of companies rendering funeral service

The Office conducted inspections into information systems of various funeral service companies. The objective was to examine if all services are performed and the personal data of their clients processed in compliance with the Act on Personal Data Protection. In some cases, it has been proven that the respective controllers of information systems do not comply with Slovak data protection law in various aspects.

Special registration for biometric personal data
By conducting an inspection in a company, a famous producer of brand electronics, it was discovered that the controller did not register its information system containing biometric data. Under the Act on Personal Data Protection, the controller is obliged to submit the information system for special registration if he intends or if is he already processing biometric data, except for the analysis of DNA and the DNA profile of natural persons for the purposes of registration or identification in entering sensitive, specially protected facilities, premises with reserved access or in accessing technical appliances or devices with a high rate of risk and in cases of solely internal needs of the controller. In this particular case, the Office imposed a significant fine of 30.000,-SKK.

Unlawful disclosure of personal data by a non-banking company providing credit loans
A company dealing with loan debt recoveries used to send an open letter reminder to its debtors by means of correspondence card with an expressive notice in colour that the addressee was a "BAD PAYER" and stating the outstanding amount. In this way, the economic situation of the data subjects was disclosed to third subjects, which was not necessary for fulfilment of the purpose of processing. The Office issued an order in which it imposed the termination of such processing of personal data on the controller. The controller did not agree with the order of the Office as the company lost its instrument for psychological constraint on its debtors. Since the controller did not lodge an objection against the order within the lawful period, the company lost the opportunity to seek effectively protection in court. Consequently, the controller lodged a motion for examination of lawfulness of the issued order to the General Prosecutor's Office of the Slovak Republic and asked for nullification of the order. As a reason, the controller stated violation of its constitutional right to free business. The prosecutor confirmed the objective correctness of the order and its justness in this case. Consequently, the controller lodged a repeating motion to the superior prosecutor and asked for the examination of the order again. The superior prosecutor also confirmed the correctness of the Office's procedure and notified the controller that he would not examine further motions in this case.

Unlawful disclosure of national identification number (birth number)
In 2007, the Office continued continuous observations of the personal data protection which focused particularly on the publication of national identification numbers "the birth number" on the Internet. Orders to remove shortcomings identified were issued by the Office to several subjects e.g. the Tax Directorate of the Slovak Republic, a football association, the Anti-Trust Office of the Slovak Republic and others.

Scanning and copying of documents without the data subject's consent
Documents may not be copied or scanned without a proper legal basis, which in Slovakia is either a Special Act, or the written consent of the data subject. Inspections of various public and private entities carried out by the Office revealed that this rule was being ignored by a vast majority of controllers. They usually conducted this kind of processing beyond the extent necessary for achieving the purpose of the processing of personal data and without the due consent of data subjects. The Office issued binding orders in this respect.

Transborder data flow
In 2007, the Office issued more than 30 official statements (explanations, interpretations of law) concerning transborder data flow within or outside the European Union. The arbitrary determination of the controller or processor status in various contractual relationships or the lack of their contractual definition obliges the Office to provide sound explanation. Employment data is that which is most wanted of the categories of personal data transferred to third parties abroad. However, the banks also require some sensitive personal data, such as the national identification number, which seems to be excessive to their service performance. They justify it through their globally interconnected and mirrored information system. The Office was asked for approval mainly by subjects of the financial (banking) sector and those transfers were also approved (in total 9 approvals). In other cases, largely incomplete grounds provided by the controllers seeking the Office's approval for the designed data transfers taking place all over the world led mostly to denials of approval. One approval was issued for a global mobile operator at the beginning of January 2008.

In order to precisely apply the respective sections on transborder data flow of the Act on Personal Data Protection, guidelines for controllers requesting approvals of the Office concerning international transfers of personal data were published on the Office's web page.

Public Opinion Poll

A public opinion poll focusing on the level of awareness in matters of personal data protection was conducted by the Opinion Research Institute of the Statistical Office of the Slovak Republic. The poll revealed that more than a half of respondents were aware of their rights related to the protection of personal data. This was the first time since 1999 that a considerable group of respondents (51%) was aware of their rights related to data protection, so awareness had increased by 31%. There was a 6% increase compared to 2005. Most aware were citizens with a university education (78%), entrepreneurs (70%), employees (65%), secondary school educated (59%), citizens living in towns with 50,000 to 100,000 citizens (59%). The least aware were citizens with elementary education (30%). A relatively high awareness varying between 57% and 59% was declared by quite a wide range of the population aged between 35 and 49 years of age.

The public opinion poll study is a complex document focused on various aspects of obligations and rights stipulated by the Personal Data Protection Act, for instance the sensitivity of personal data regarding the possibility of misuse, photocopying original ID documents, trust of citizens towards various data controller groups, personal data transfers to third countries, threats of misuse of personal data communicated via Internet, consent of citizens with authorised phone tapping or Internet communication monitoring as part of the fight against terrorism. The details of the analysis may be found in the Annual Report for the year 2007 of the Office published on our web pages www.dataprotection.gov.sk .

International cooperation

On 21 March 2007, the second evaluation mission Sch–Eval of the European Commission visited Slovakia. The Office was examined together with other relevant authorities.

The evaluation mission came with the purpose of evaluating the implementation of the recommendations given by the first evaluation mission in February 2006. The subjects of evaluation were as follows:

1. Legislative framework for the implementation of SIS (Schengen Information System), specifically SIS one4 All;
2. Competences, capacity and functionality of the Office;
3. Schengen visa issuance procedures;
4. Information to the general public about data subjects' rights enforcement concerning the processing of their personal data within the Schengen Information System and about the changes undertaken with regard to the entering of the Slovak Republic into the Schengen area.

The Office has proven capability to fully perform its competences to inspect police databases. Slovakia joined the Schengen area one minute after midnight on 21 December 2007.

Within the framework of building up partnerships with central and eastern European data protection authorities, in addition to the annual Central and Eastern European Commissioners Conference which took place in Zadar in 2007, two days of negotiations were held with deputies of the Romanian DPA in April 2007 in Bratislava, where the main issues of personal data protection, including the conditions met and steps to be taken for full accession of the Slovak Republic to the Schengen area, were discussed. Both DPAs concluded an agreement on cooperation.

Within the international project aimed at creating and enhancing the effectiveness of the activities of the Directorate for Personal Data Protection and Data Protection Enforcement of the former Republic of Yugoslavia–Macedonia, one employee from the Office's department of foreign relations took part in the project as the short term expert for information technologies and security. In June 2007, this representative of the Office was elected chairman of the Joint Customs Supervision Body for the Customs Information System.

Slovenia

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

The Personal Data Protection Act adopted on 15 July 2004 (hereinafter PDPA)[10] by the National Assembly of the Republic of Slovenia was amended in 2007. With the adoption of the Personal Data Protection Act, Information Commissioner Act and the establishment of the Information Commissioner, full implementation of Directive 95/46/EC to the Slovenian legal order was ensured.

The Personal Data Protection Act was amended in 2007 by the Act on Changes and Amendments to the Personal Data Protection Act, which was adopted by the Parliament of the Republic of Slovenia on 12 July 2007[11]. According to the amendments, all the data controllers with fewer than 50 employees (previously 20 employees) are not required to fulfil the obligation laid down in the second paragraph of Article 25 of the Personal Data Protection Act (obligation to prescribe in their internal acts the procedures and measures for security of personal data and to define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data) and are not required to fulfil the obligations laid down in Articles 26 and 27 of the Personal Data Protection Act (establishment of a filing system catalogue for each filing system and obligation to notify the national supervisory body – Information Commissioner about the establishment of a filing system or prior to the entry of a new type of personal data in existing filing system). These exemptions however do not apply to filing systems kept by data controllers in the public sector, notaries public, attorneys, detectives, bailiffs, private security providers, private healthcare workers, healthcare providers, and to data controllers that keep filings systems containing sensitive personal data and for whom processing of sensitive personal data is a part of their registered activity.

Furthermore the time period for the frequency of filing a request for access to information was changed (Art. 31 of the PDPA). According to the amendments, such requests may be lodged similarly to the procedure before the amendment: once every three months, and in respect of sensitive personal data and personal data under the provisions of Chapter 2, Part VI of this Act (data processing related to video surveillance), once a month. But the amendment added the provision that, when required to ensure fair, lawful or proportionate processing of personal data, particularly when an individual's personal data in a filing system is frequently updated or sent or could be frequently updated or sent to data recipients, the data controller must permit the individual to lodge the request within an appropriately shorter period, which is not less than five days from the day of acquainting with personal data that relate to him or (from the) refusal of this acquaintance.

The Amendment further specified that as a rule the data controller must enable the individual to consult, transcribe, copy and obtain a certificate pursuant to subparagraphs 1 and 2 of the first paragraph of Article 30 of this Act on the same day that the request is received (previously no later than 15 days from the day of receipt of the request), and no later than within 15 days, or within 15 days to inform the individual in writing of the reasons why he will not enable consultation, transcription, copying or the issuing of a certificate.

Additionally, provisions on material costs with regard to requests for access to information which the data controller may charge to the individual for the transcription, copying and written certificate, the extract, the list or the information from Items 5 and 6 and the explanation from Item 7 of the first paragraph of Article 30 of this Act. The data controller may charge the individual only material costs according to a pre-specified tariff (issued by the minister responsible for justice, at the proposal of the Information Commissioner), while an oral confirmation, oral provision of information and oral explanation are free of charge. If despite having received an oral confirmation, information or explanation an individual requests confirmation, information or an explanation in written form, the data controller must provide it.

[10] Official Gazette of the RS, No 86/2004.

[11] Official Gazette of the RS, No 67/2007.

With the amendments also all the fines related to violations of the Personal Data Protection Act were changed to euro currency.

In 2007, the Information Commissioner regularly participated in five EU working parties, which deal with personal data protection and joined the Member States' personal data protection institutions (Working Party 29, Joint Supervision Body of Europol, Joint Supervision Authority of Schengen, Customs Joint Supervision Authority and EURODAC Supervision EDPS - DPAs Coordination meeting dealing with processing of personal data in different contexts in the EU). Within Working Party 29, the Commissioner also has a representative in one sub-group – ITF.

The Slovenian legal order implemented Directive 2002/58/EC through amendments to the Electronic Communications Act[12], adopted on 9 April 2004, and valid from 1 May 2004. Chapter X 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[13], which implemented the Directive 2006/24/EC 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, email, telephone, mobile telephone, etc.) need to retain, for the period of two years, all traffic data created through their customers' activities. The Act's provisions regarding the retention of telephone data entered into force on 15 September 2007, while the provisions regarding the retention of internet access, email and VOIP data are scheduled to do so on 15 March 2009.

In 2007, the Information Commissioner participated in the inspection team conducting the annual inspection of Europol by the Joint Supervision Body of Europol. The Commissioner conducted an inspection of the national Europol unit.

[12] Official Gazette of the RS, No 43/2004 and 86/2004.

[13] Official Gazette of the RS, No 129/2006.

The Information Commissioner is also required to carry out supervision over 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 defines conditions under which biometric measures are to be allowed. The performing of biometric measures is allowed only after the receipt of the supervisory body's decision granting the performance of biometric measures.

Significantly, a growing trend was noted in 2007 in the number of related applications. In 2007, the Commissioner received 40 applications of which 31 were from the private sector and 9 from the public sector (compared with 15 applications in total in 2006).

In 2007, the Information Commissioner issued a total of 35 decisions regarding the execution of **biometric measures**, 24 of which granting the execution of biometric measures. Requests to grant the execution of biometric measures were rejected in two cases, in another case sustained in part, and refused in a further ten cases. The Commissioner granted the use of biometric measures for the entrance to premises where protected programme equipment is stored and to areas where documentation containing company trade secrets and other protected information is stored. The Information Commissioner refused an application for granting the permission of execution of biometric measures over employees merely for the reasons of recording presence at work.

There was also an increase in the granting of permits for the **connecting of filing systems**. In 2007, the Information Commissioner received 12 applications (7 in 2006) for the connecting of filing systems. The Commissioner issued a total of 7 decisions regarding the connecting of filing systems.

Generally, according to the PDPA, the controller of personal data needs an adequate legal basis or personal consent of the individual to whom the personal data relates for any processing of this data and for publishing

of this data in the media. However, if in accordance with the principle of proportionality, the constitutionally guaranteed right to know prevails over the right to personal data protection, the publication of such personal data could also be legal. As no specific exemptions for the media is stipulated by PDPA, the implementation of personal data protection and thus the provisions of PDPA with relation to the constitutionally guaranteed right to freedom of expression (implemented in practice through the Public Media Act[14]) needs to be interpreted as requiring the media to respect PDPA and thus respect the principle of proportionality as defined in Art. 3 of PDPA. In 2007, the Information Commissioner conducted several procedures against the media who were violating the provisions of the Personal Data Protection Act.

1. A journalist from one of the main TV stations published in a daily evening news programme in non-anonymised form the content of a criminal complaint and by doing so published the following personal data of the denounced persons: name, date of birth, address and unique personal identification number. The offender had no legal basis or personal consent of the affected individuals for the publication of this personal data neither was this a case of prevalence of the right of the public to know about the published personal data. The published personal data was not adequate in extent according to the purpose for which it was published which represents a violation of the proportionality principle. The violation was committed by the processing of the personal data, namely dates of birth, addresses and unique personal identification numbers of three individuals were published illegally. The journalist immediately withdrew the disputed news item from the website and prevented further violations.

2. The Information Commissioner established in the inspection proceeding a violation of the PDPA committed by the publishing of an identity card revealing the following personal data of the individual: photo, name, date of birth, place of birth, unique personal identification number, sex, number of identity card, place of issue and issue and expiry date of the identity card and signature. Since the individual concerned was not a public person *par excellence* the media did not have the right to interfere with his privacy without limitations. Details from his identity card are clearly not important for public debate about issues which are of general or public interest. The Commissioner further established in a specific case that, from the perspective of public interest, to be informed of current affairs and also to issue a search warrant the purpose of which is to bring or arrest the person charged, it suffices to reveal certain personal data of the individual concerned (photo and name) but not all data. By publishing only a limited scope of personal data, the public would receive all the information it needs to be properly informed. All the other personal data of the individual concerned is not important information in relation to the public interest and freedom of expression as individuals can be identified by published photos with full written names.

According to the proportionality principle, there were no adequate legal grounds allowing publishing of the above mentioned published personal data of the individual concerned, therefore the publishing of this data on the website meant violation of Art. 3 of PDPA. The published personal data was not proportionate to the purpose for which it was published.

The media has, after being served the regulatory decision of the Commissioner, within a set deadline, removed the found irregularities and prevented further violations.

3. Similarly, as in the above mentioned case, and for the same individual, another media company published the above mentioned personal data of this individual: photo, name, date of birth, place of birth, unique personal identification number (EMŠO), sex, number of identity card, place of issue and issue and expiry date of the identity card and signature on their website. For the same reasons as mentioned above, under item 2 and after the regulatory decision of the Commissioner, the media similarly removed the published excessive personal data from the website.

4. The Information Commissioner, in another case in the inspection proceedings, established a violation of PDPA committed through the publishing of photograph of a passport in the printed version of a newspaper thus publishing the following personal data of the owner of the passport: photo, name, citizenship, date of birth, sex, place

[14] Official Gazette of the RS, No 110/2006.

of birth, issue and expiry date of the passport, number of the passport, unique personal identification number (EMŠO), issuing authority and signature. The processor did not have the legal basis for such processing – publication of this personal data (neither in law nor through the personal consent of the individual concerned) nor was this a case of the overriding right of the public to know which would allow publishing of all the published personal data. Similarly, as in the above mentioned cases, the published personal data was also in this case not proportionate to the purpose for which it was published.

5. The daily newspaper published a criminal complaint filed by police against a private individual thereby processing illegally by publishing the following personal data: name, date and place of birth, address, citizenship and unique personal identification number (EMŠO). The Information Commissioner also established a violation of PDPA committed with the publishing of the above mentioned personal data without adequate legal basis or the personal consent of the individual concerned.

In 2007, the Commissioner issued **several decisions widely publicised by the national media**, two in particular:

1. The Information Commissioner initiated inspection proceeding against all Slovene pharmacies and insurance companies offering voluntary health insurance due to the public polemic about the disagreement between different pharmacies and the Vzajemna health insurance company. In its decision, the Commissioner interpreted the means of how the personal data related to voluntary health insurance should be transferred, since transfer of personal data was also the subject of a dispute between pharmacies and insurance companies. As was established during the inspection procedure the following personal data of insured individuals are exchanged between insurance companies and pharmacies: number of the health insurance policy, number of the health insurance card, date of birth, sex, name or code number and quantity and date of the issued medicinal product or medical devices.

The health insurance companies are entitled to obtain personal data on the basis of existing legislation. The Commissioner stressed, in particular, that the insurance companies (as well as all the other controllers of data filing systems including pharmacies in this case) need to handle the data in conformity with the purpose for which they collected them (in this case personal data could only be used for balancing schemes and settlement of loss events and with the pharmacies only for transferring the data to the insurance companies and for supervision over the correctness of their settlements and for potential other purposes defined by another law). In particular with insurance companies this data is not allowed to be included in any other data filing system related to other insurance transactions.

A legal obligation to transfer personal data exists according to Para. 1, Art. 22 of PDPA, therefore the controllers (pharmacies) have to send this data and do not have a discretionary right to decide otherwise. The pharmacies and insurance companies must not use potential inadequate (too low) compensations for transmission to the detriment of the public interest of the Republic of Slovenia and of the insured individuals. They are especially not allowed to neglect their duty to protect personal data, for example, by sending them in a non-secure electronic form or, contrary to the law, shift the burden for acquiring compensation for the paid medications and transmission of personal data to the insured individuals (by asking them to individually provide the insurance companies with these receipts). Furthermore, the law is clear in stipulating that the data may only be transferred from pharmacies to insurance companies.

The disputed costs of this service which the pharmacies are providing to the insurance companies might of course be subject to other legal proceedings, but since the law clearly stipulates who has the obligation of transferring the data, actual transfers cannot stop while these disputes are being resolved. As the transferred data includes sensitive personal data (on the health status of the individual), the Commissioner decided that the data should be transferred in encrypted form using electronic signature, ensuring that it is unreadable and unrecognisable.

One of the liable subjects has filed an appeal against the Commissioner's decision. The court ordered, in an administrative dispute, that the Commissioner's decision be annulled.

2. The Information Commissioner received several complaints from individuals about receiving open pre-completed tax declaration forms or forms which were poorly sealed allowing anyone to examine the tax-related information contained in them. The Commissioner has initiated the inspection procedure against the Tax Administration of the Republic of Slovenia and their responsible person(s) relating to establishing the adequacy of protection of personal data during the dispatching of pre-completed tax declaration forms and the violation procedure against their contractual processor.

Both the agency and its contractual processor have committed the violation of not providing adequate protection of personal data during the dispatching of the tax declaration forms which made it possible for non-authorised persons to examine and thus process the personal data concerned. The agency is, according to Art. 24 and 25 of PDPA, as the data processor liable to ensure protection of the personal data from their data filing systems also during their transmission to other users or during the transmission of tax forms to each taxable person. This includes the obligation of the agency to ensure that any documentation containing sensitive personal data of taxable persons (confidentiality of tax related data) is dispatched in envelopes which firstly prevent third persons from examining the data enclosed without visible damage to the envelope and secondly which is printed in such a way preventing third persons from seeing its content (including personal data) by normal light.

The Tax Administration of the Republic of Slovenia has corrected the mistake and stopped further dispatching of the pre-completed tax declaration forms immediately after receiving the complaints from individuals. All further consignments after that were additionally secured by plastic foil and additionally sealed thus ensuring adequate protection of the pre-completed tax declaration forms.

In 2007, the Information Commissioner **lodged two requests for a judicial review**:
During her tenure, the Information Commissioner has lodged applications for a constitutional review of certain provisions of four statute laws (2 in 2007) and contributed to the preparation of many different pieces of national legislation from the point of view of personal data protection.

1. In 2007, the Constitutional Court passed a decision[15] on the request for a 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[16] lodged by the Commissioner in December 2006. The Court granted the request of the Information Commissioner in part pertaining to the publicity of the real estate register and to physical persons (data on owner, user, tenant and manager of the real estates - their name and unique personal identification number – EMŠO) which was the main complaint put forward by the Commissioner against the legislator. The publicity of the real-estate register would allow publication of the personal name of the individual and their unique personal identification number in connection with the real estate. As these would be available on the internet that would enable collected personal data to be used for any purpose whatsoever, which the court established to be inconsistent with the constitution. The court confirmed with its decision that by publishing the real estate register irreparable damage would be done to the individual.

2. A judicial review of Item 7, Paragraph 2, Article 62 and Paragraph 2, Article 62d of the Health Care and Health Insurance Act[17], regulating processing and transmission of data necessary for implementation of the countervailable schemes and Article 2 of the rules concerning implementation of supplementary health insurance which providers of health services are requested to follow[18]. The Commissioner argued that the challenged provisions of the Act are in contradiction of Art. 38 of the Constitution of the Republic of Slovenia with regard to the requested specification of the type of personal data to be processed. The challenged provisions of the Act stipulate a general clause and duty to transmit all necessary data or all data necessary for the implementation of the countervailable schemes. Existing legal regulation does not specify types of personal data to be processed which

[15] Official Gazette of the RS, No 65/2007.
[16] Official Gazette of the RS, No 47/2006.
[17] Official Gazette of the RS, No 72/2006 and 91/2007.
[18] Official Gazette of the RS, No 7/2007.

leads to different interpretations and thus potentially to disproportionate processing of personal data. This is in contravention of the constitutional principle of proportionality which stipulates that any interference into the constitutionally protected right has to be proportionate to the goals which such interference defined by the law aims to achieve. Equally defining the scope and types of collected personal data by a sub-legal regulation (not by a statute) is unconstitutional. The legal definition which stipulates that "all necessary data" should be transmitted is not fixed and therefore does not define specifically enough the processing of personal data as required by Art. 38 of the Constitution as it gives too broad authorisation for regulation of processing of personal data to a sub-legal regulation.

3. Judicial review of Paragraph 4, Article 47, Indent 1, Item 1, Paragraph 2, Article 58, Item 5, Paragraph 1, Article 123, Items 3 and 4, Article 165, Item 2, Paragraph 2, Article 247, Item 3, Paragraph 1, Article 334, Item 3, Paragraph 1, Article 432 and Item 1, Paragraph 1, Article 543 of the Market in Financial Instruments Act[19] which are according to the opinion of the Information Commissioner in contradiction of Art. 38 of the Constitution of the Republic of Slovenia due to lacking specification of the type of personal data to be processed.

The disputed law specifies neither the purpose nor the scope of personal data to be collected or processed. The challenged provisions of the law stipulate only processing of personal data but do not provide specification which personal data are to be processed. This leaves open the question of the scope of personal data to be processed and collected to the potentially arbitrary decision of the securities market agency. The existing legal regulation is referring the definition of this area to sub-legal regulation which is in contravention of the constitution. The scope and type of personal data should be entirely regulated by law.

The existing openness and lacking specification of the legal basis which defines the processing of this personal data could lead to different interpretations and therefore to disproportionate processing of personal data. This is in contravention of the principle that any measure i.e. the scope of impairment of the protected value or good should be proportionate to the value of aims defined by the law. Therefore the legitimate interference with certain right should be diminished to the minimal level still ensuring achievement of the defined aims and thus establish reasonable balance between the value of these aims and the gravity of the encroachment upon someone's right.

[19] Official Gazette of the RS, No 67/2007 and 100/2007.

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, that is, to adopt a decision on video surveillance execution, publish an appropriate notice, inform its employees in writing, obtain the consent of apartment buildings co-owners, consult the syndicates, etc. Many of the video surveillance controllers however still failed to adjust their practice to the provisions of the law which led to a number of appeals filed with the supervisory body.

Several reasons for suspected violations of the PDPA were also in relation to illegal collection of personal data such as: collection of personal data with regard to participation in different gaming competitions, in relation to contracts with the telecommunication operators or in relation to supervision of the employees by the employer. Other areas of suspected violations of the PDPA were also: direct marketing, the area of illegal publishing of personal data (on different information displays in residential buildings, at the workplace), inadequate protection of personal data and transmission of personal data to unauthorised users. Important areas where the inspections showed significant inadequacies are: non-existence of a legal basis for processing (in law or personal consent of the data subject), inadequate protection of personal data, failure to implement reporting of the data filing system to the register, processing of sensitive personal data.

By the end of 2007, some 10,000 personal data controllers reported data on personal data filing systems they manage (after the amendments to the PDPA in 2007 the number of controllers obliged to report data on personal data filing systems they manage decreased significantly). 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.

Inspection activities (as of 1 December 2007, there are eleven supervisors employed by the Commissioner): In 2007, the Information Commissioner received **406** (179 in the public and 227 in the private sector) applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act; compared with **231** cases (88 public and 143 private sector) in 2006. The increase amounts to 76%. Most complaints pertained to disclosure of personal data (hereinafter PD) to unauthorised users, unlawful or excessive collection of PD, illegal video surveillance, insufficient PD protection, unlawful publication of PD etc. Accordingly, a significant increase has been noted in the initiated administrative offence procedures: 133 cases in 2007 compared with 41 cases in the previous year.

The number of requests for **written opinions and clarifications** received by the Information Commissioner has also significantly increased from 616 in 2006 to 1144 in 2007 (or even compared with just 34 cases in 2005!). This undoubtedly reflects a growing public awareness of the right to privacy brought into effect by a modern Personal Data Protection Act and is, hopefully, also related to the transparent work and intensive public campaigning performed by the Information Commissioner.

Spain

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

European Parliament and Council Directive 95/46/EC was incorporated into Spanish legislation in the Organic Act 15/1999, of 13 December on the Protection of Personal Data.

1. Royal Decree 1720/2007, dated 21 December, which approves the Regulation implementing the Organic Act 15/1999 on the Protection of Personal Data

The approval of this regulation is a milestone in Spanish data protection legislation. It intends to guarantee the necessary legal certainty in an area as sensitive for fundamental rights as that of data protection, consolidating the precedents established by the Spanish Data Protection Agency. It also intends to resolve the most frequently asked questions, and problems with interpretation that may currently exist, paying particular attention to those that may be of greater significance. Comments and observations from the current authorities of the autonomous communities have been taken into account, as well as those of more than sixty entities and associations representing the rights and interests affected by this regulation.

The regulation expressly includes within its scope of application non-automated files and processing of data (on paper) and sets out specific criteria regarding their security measures. It also regulates the territorial scope of application, establishing that all processing is subject to this regulation if Spanish legislation is applicable, according to the rules of public international law, or when means located in Spanish territory are used, unless solely for transit purposes.

Of particular significance is the incorporation of the authorisation for the processing of data as necessary for the purposes of the legitimate interest pursued by the data controller.

Similarly, it regulates a procedure for guaranteeing that any person may have full knowledge of the use of such data, before consenting to his data being collected and processed. In addition to this, of particular importance is the establishment of specific rules relating to the provision of consent by minors, which will demand the assistance of their parents or guardians when the child is less than 14 years old.

In the pursuit of a better guarantee of the right of persons to control the accuracy and use of their personal data, the data controller is expressly required to provide data subjects with a free and simple means of allowing them to exercise their right of access, rectification, erasure and objection. Along the same lines, it is prohibited to demand the data subject to send registered letters or similar, or use telecommunication means that imply the payment of an additional charge. Finally, although the regulation is not applicable to deceased persons, to avoid painful situations for their relatives, it provides that they may inform the data controller of the death and request cancellation of the data.

The applicable rules to data processors are also regulated in detail. Another novelty is the establishment of a detailed system for processing regarding, on the one hand, financial solvency and creditworthiness, and on the other, advertising and commercial research activities, implementing the specific provisions contained in the Organic Act 15/1999.

Regarding international transfers of data, the regulation establishes a systematic regime for this, acknowledging the possibility that the Director of the Spanish DPA may declare the existence of an adequate level of data protection in a country where such a declaration by the European Union does not exist, clarifying situations in which guarantees may be provided which permit authorisation of a transfer by the Director, and including the so-called "binding corporate rules" or internal codes of multinational groups of companies. Finally, the regulation establishes the procedures that the Spanish Data Protection Agency should handle for the performance of its functions, and expands the duty of the Spanish Data Protection Agency to collaborate with the data protection authorities of the autonomous communities.
https://www.agpd.es/upload/English_Resources/reglamentolopd_en.pdf

2. Organic Act 10/2007, of 8 October regulating the police database on DNA identifiers

Upon signing the Treaty of Prüm in May 2005, it was necessary to merge the police databases containing genetic data that were valid in Spain until that time. The purpose of this Organic Act was the regulation of the police databases containing identifiers obtained from DNA during criminal investigations. These identifiers will only provide genetic information regarding the

identity of the person and their gender (non-coding DNA). Similarly, it regulates the guarantees that shall be applied for the transfer of such information to authorised security forces, as well as the duration of storage. This information shall only be used by the authorised bodies and for criminal investigations. Data shall be kept until the Statute of Limitations is applicable to the crime.

3. Act 37/2007, dated 16 November on re-use of public sector information

This act transposes the Directive 2003/98/EC to Spanish legislation. It applies to documents that the public sector could make accessible for re-use by citizens or companies in order to exploit the possibilities that this kind of information may allow, with a view to contributing to economic growth and job creation, and to increase the transparency of the public sector too. As the directive lays down, this act does not alter the obligations and rights set out in the Spanish Data Protection Act.
http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/19814 (in Spanish)

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 incorporated into Spanish legislation by the State Telecommunications Act 32/2003, of 3 November, implemented by Royal Decree 424/2005, of 15 April, which regulates the conditions for the provision of electronic communications services, universal service and the protection of users.

1. Act 25/2007 of 18 October on retention of data relating to electronic communications and public communication networks

This act, a transposition of the Directive 2006/24/EC on the retention of data, establishes the storage of data on electronic communications for twelve months, for public safety purposes. Information regarding unsuccessful calls and pre-paid cards shall also be stored. The transfer of this information to security forces shall be done following a court order and only to authorised agents.
http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440 (in Spanish)

2. Act 11/2007 dated 22 June on electronic access by citizens to public services

The purpose of this act is to enhance the use of electronic means in the government-to-citizen relationships, improving the universal accessibility to the information and services provided by the public administrations, and the interoperability between the different administrative bodies. It establishes that the availability of the use of this kind of means, in a secure and comprehensible way, is a right of the citizens, and a correlative obligation for the administrations. The processing of data, as is natural, must respect the obligations and rights set down in the Spanish Data Protection Act, guaranteeing the use of the data obtained by electronic means for the precise purpose for which it has been sent to a specific administrative body.

As a result of this act, the Official Spanish Gazette and other official journals will be published in electronic editions. Likewise, due to its nature as a basic law, it is being developed by the autonomous communities (e.g. Decree 232/2007 of the Autonomous Community of the Basque Country, dated 18 December).
http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/12352 (in Spanish)

3. Act 56/2007 of 28 December on the Measures for Promoting the Information Society

This act establishes some novelties regarding electronic billing and contracting processes in electronic commerce in order to ensure the relations between users and consumers and the electronic services providers, who must guarantee the respect of Spanish data protection legislation rules in their processing of data.

Additionally, the companies that provide some services with a special economic relevance should facilitate the exercise, by the data subject, of the rights of access, rectification, erasure and objection by electronic means.
http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440 (in Spanish)

B. Major case law

An analysis of the degree of legal security in the application of LOPD makes it necessary to consider the extent to which the decisions of the AEPD are ratified or revoked in court. The Court for Judicial Review of the National Court has passed 158 judgments, and the Supreme Court has passed 13 judgments and two writs of non-acceptance. Below are the most salient of these:

1. National Court

- Mass remittance of spam.
- The judgment of 25 October 2007, confirming that the publication of the personal data of a citizen in a corporate means of dissemination without his consent infringes the right to data protection.
- The judgment of 14 November 2007, which interprets that the data protection regulations and the patient autonomy regulator do not make it obligatory to return diagnosis tests.
- The judgment of 19 December 2007, which analyses the clash between two fundamental rights, that of freedom of trade union affiliation and the protection of personal data, granting preference to the former.
- Sentence of the Spanish Supreme Court on Apostasy. The decision of the AEPD on the right of citizens not to appear in the Register of Baptisms and to exercise their right of cancellation of these files was appealed by the Archbishop of Valencia before the National Supreme Court. The decision of this body upheld that of the AEPD. The following aspects of this decision must be emphasised: Registers of Baptisms are deemed personal data files in the sense of the LOPD; failure to erase such data may constitute a breach of the principle of quality of data.

2. Supreme Court

It is necessary to stress that the Supreme Court has ratified the criteria of the AEPD on 11 of the 13 occasions on which this matter was submitted to its consideration.

In particular, the following Supreme Court judgments must be referred to:

- The judgment of 16 February 2007 rejects the appeal lodged against the Judgment of the National Court which in turn rejected the appeal seeking the cancellation of Instruction 1/1995 passed by this agency. The judgment of the Supreme Court understands that the agency may pass instructions in order to arrange the actions of operators in terms of automated processing so that they are suited to the principles established by law, in a compulsory manner and with an *ad extra* effect, in similar terms to those acknowledged for other regulators by the same court.
- The judgment of 27 March 2007 confirms the agency's criterion of deeming contrary to the LOPD the assignment by a (telecommunications) operator of data on its customers to a third-party entity so that the latter may conduct a scoring of their financial solvency.
- The Judgment of 17 April 2007 considers in conformity with the law the penalties imposed by the AEPD on a number of entities that took part in the process of selecting participants for a certain television program, because a number of assignments took place, some of them relating to the health of the participants, and because the security measures that should be required by data protection regulations were not adopted.
- The Judgment of 12 December 2007 considers in conformity with the law the criterion of the AEPD of resolving that there was an unlawful processing of data relating to the health of individuals in cases of hiring by the entrepreneur of an entity to check the source of absenteeism among his employees.

3. Resolutions by the Spanish DPA

During 2007, the number of claims filed by citizens with the AEPD rose by around 7% to a total of 1,624. The number of investigations commenced by the AEPD, owing to claims or *ex officio* at the director's initiative totalled 1,263. On the other hand, in 2007 the AEPD resolved a total of 399 penalty procedures, representing a 32.5% increase over the previous year. In relation to declared penalties, the fines imposed by the AEPD amounted to 19.6 million euros.

There was a very strong increase in the applications for the protection of rights, there being a 54% increase of those which were accepted (879 in total). These applications for the protection of rights show the same concerns as stated above, and the rights that were protected most often were those of erasure (62%) and access (32%).

The right of cancellation of data of 2007 was strongly influenced by a specific phenomenon relating to the cancellation of data in the Baptism Books of the Catholic

Church; of the 896 procedures for the protection of rights that were commenced, 34% (304) were for that purpose.

Together with this, the applications for cancellation submitted by citizens have mainly referred to the following matters:

- Undue inclusion of their data by financial institutions in information files on solvency and creditworthiness, as well as the cancellation thereof at the end of the legal relationship with said institutions;
- Removal of data from the files of telecommunications operators in cases of a change of telecommunications operator not consented to by the subscriber;
- Cancellation of data on the Internet (forums or message boards, YouTube);
- Access to clinical histories.

In terms of penalties by sectors, the top spot was for the telecommunications sector, with 112 procedures resolved, followed by financial institutions (80) and marketing communications and spam (37). Below are some of the most relevant resolutions.

- **Video-surveillance:** The AEPD began an *ex officio* investigation into the capture and dissemination via YouTube of images of a street in Madrid, in order to clarify whether there had been a breach of the LOPD regarding the capture using video cameras and later dissemination through YouTube, possibly having committed serious or very serious breaches of the data protection legislation, punishable with penalties of up to € 600,000.
- **Emule:** The AEPD imposed a penalty on the leakage of personal data on the Internet through the Emule file-sharing system. This is the first penalty by the AEPD for using systems which permit the sharing and downloading of text, video or music files, among others, that are stored in the computers of other users. The AEPD requires the implementation of security measures such as firewalls, and the careful selection of the directory containing the information that is to be shared.
- **YouTube:** the AEPD began an *ex officio* investigation into the capture and dissemination through YouTube of images of a disabled person, protecting the right of cancellation of the data subject's representative, possibly constituting a very serious breach of the LOPD by processing and later disseminating data images relating to the person's health.
- **Internet Forums**: the Spanish Data Protection Agency resolved that the right of erasure also applies over personal data published on an Internet forum, when the data subject is not a celebrity nor is involved in a relevant fact. The disclosure of personal data on the Internet is not always protected by the freedom of expression.

C. Major specific issues

1. Transparency

Before Parliament

Appearance of the director of the agency before the Lower House of the Spanish Parliament

In his annual speech, the Director of the AEPD emphasised the recent proliferation of video-surveillance devices, not only by public authorities but mainly in the private sector, through the generalisation of camera-installation initiatives, for example, in owners' associations, commercial premises or transport services.

He also referred to services such as "YouTube" which permit the global dissemination of images to all Internet users.

In his speech he also referred to the need to offer guarantees in light of the new risks arising from Internet services such as "search engines and e-mail services," reminding that search engines must guarantee the effective exercise of the rights of access, rectification, cancellation and objection.

2. Co-operation with the data protection agencies of the autonomous communities

The acquired experience, together with the process of re-signing of some statutes of self-government, has led to a reflection on the convenience of establishing a new co-operation model between the existing data protection agencies. To this end, five working groups have been established (Registration; Inspection; Legal and Regulatory Analysis; Organisation, Communication and Modernisation; and International). The measures that have been cited in the aggregate reinforce the bases to guarantee the equality of all citizens in

respect of the fundamental right of the protection of personal data. It simplifies the obligations of the file managers and increases the efficiency of the agencies' activities.

3. Recommendations to the Government

During 2007, the AEPD made a number of recommendations especially aimed at the public authorities. Among these, regulatory developments are proposed for:

- Carrying out procedures allowing the protection of copyright in a manner compatible with the fundamental right to data protection;
- Regulating the anonymous publication of judgements by jurisdictional bodies;
- Regulating the internal reporting systems available to workers in companies, specifying the activities in which it might be necessary to establish these systems, guaranteeing confidentiality for the reporting party and the rights of the reported parties.

Also, the AEPD has made a number of executive recommendations stressing the need for the relevant public administration to carry out the following actions:

- A plan for the protection of data of minors on the Internet: public authorities are to be required to articulate specific plans for the protection of minors on the Internet;
- Fostering of precautions to prevent the undesired exchange of sensitive personal data on the Internet via P2P networks;
- Encouraging self-regulation in the media to guarantee privacy and the protection of personal data; encouraging practices that are more respectful towards the data protection regulations;
- Actions for guidance on the use of confidentiality guarantees of recipients in the remittance of emails;
- A Plan for the Fostering of Good Practices in the guarantee of privacy in Official Gazettes and Journals, by means of the adoption of measures that, while not affecting the actual purpose of official journals, are able to limit the capturing of personal information by search engines on the Internet;
- A local strategy aiming to adapt the installation of traffic control cameras to the regulations on the protection of personal data.

4. More information, more awareness, more queries

Information is a key item in terms of fostering awareness of the protection of personal data among citizens. Bearing this in mind, and with the purpose of meeting the growing demands of information and extending the institution's public dissemination actions, the agency has intensified its relations with the media, increasing its staff and the material means allocated to dissemination. This greater awareness has led to a substantial increase in the number of queries submitted to the Citizen Attention Service, which rose by 30% during the last full year (to a total of 47,741 queries).

5. Enforcement

A greater awareness of the data protection regulations among data subjects has led to an increase in the number of claims lodged because of alleged breach of the LOPD. The legislator has attributed to the AEPD a set of powers that allow the agency to act independently, investigating violations and imposing penalties, with the objective of guaranteeing the effective application of the regulations in force. The greater part of the inspections carried out have to do with telecommunications and financial institutions, followed by video-surveillance, which is now in third place following an increase by over 400%.

5.1 Enhancement of preventive actions

a. *Plan for the protection of the personal data of minors on the Internet*

   The Regulation for the Development of the Organic Act on Data Protection has established the basic rules for processing the personal data of minors. However, passing a regulatory framework is not enough. The establishment of programs for the control of contents, assistance to parents and to the holders of activities on the Internet and the fostering of security on the Internet requires determined actions on the part of the public authorities, articulated in specific plans for the protection of minors.

b. *Declaration on search engines*

   In 2007, the Spanish Data Protection Agency published a statement with its main observations relating to the adaptation of the policies on the collection,

retention and use of personal data by Internet search engines to Spanish data protection legislation. This report, available on the AEPD website, includes the main conclusions of the analysis carried out on the effect these practices may have on the privacy of users of the search systems and other services offered by these companies.

Conclusions:

- Search engines must bring into line the storage time limits minimising the risks to the privacy of users;
- The information provided to users is complex and inefficient;
- Citizens have the right to cancel and object to their data appearing as the result of carrying out a search.

The report may be accessed through this link:
https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/declaracion_aepd_buscadores_en.pdf

c. *Ex officio Sectoral Inspection in Colombia*
This inspection was carried out on companies making international transfers of personal data for the provision of services related to telemarketing or customer service centres. Key issues are the development and increase registered by the AEPD over the last few years in requests for international data transfers, their destination countries and main purposes for which they are requested.

The report and its conclusions can be found at the following link:
https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/report_Inter_data_transfers_colombia_en.pdf

6. Activities of Spain in the Ibero-American Data Protection Network

2007 was a particularly active year within the scope of the Ibero-American Data Protection Network, established in 2003 as a result of the AEPD initiative to promote the regulation of data protection in Ibero-America. The 5th Ibero-American Meeting took place in 2007 in Lisbon (Portugal). A seminar in Cartagena de Indias (Colombia) was also held in 2007, with the objective of creating a forum for debate and exchange of information. Guidelines were established to promote initiatives that permit the achievement of an adequate level of data protection in the countries comprising the Ibero-American Community, thus avoiding the current obstacles to the free movement of personal data in such countries. As part of its commitment to these countries, the AEPD welcomed representatives of Mexico, Chile and Uruguay to its headquarters; the latter were advised on their Data Protection Bill.

Sweden

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

The EC Directive 95/46 was 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, as the Directive, to automated processing as well as manual processing. Even though the act, in principle, applies to processing of personal data in all sectors of society, there are specific acts and ordinances that apply to processing of data in certain activities, either instead of or in addition to the PDA. Also in drafting these specific acts and ordinances, the directive has been taken into account.

In preceding Annual Reports of the Article 29 Working Party, the proposed so-called *misuse model* has been described, that is the amendment of the PDA, which entered into force on 1 January 2007. The amendment aims at – within the framework of the directive – simplifying the rules in everyday processing of personal data. This concerns such processing as typically does not lead to any greater risks of infringements of the data subject's privacy. The handling rules – the rules on notification and information, the rules of protection regarding processing of sensitive data as well as the requirement for consent in certain cases – need not be complied with when processing personal data that does not form part of nor is intended to form part of a set of personal data that has been significantly structured in order to facilitate searches for or compilations of data. So for unstructured processing, for instance regarding an e-mail message or continuous text on a website, the controller is no longer obliged to follow all the handling rules. The *misuse rule* applies instead and this rule means that the processing may not be carried out if it would result in an infringement of the data subject's personal privacy. If the misuse rule is violated then the rules on liability to damages will apply and in certain cases also penalty sanctions. The distinction between what shall be deemed as structured processing and unstructured processing can of course give rise to problems concerning the application. However, we believe that the amendment is an adaption to reality.

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.

In April 2004, the government decided to set up a Committee (*Integritetsskyddskommittén* – Committee on the protection of privacy) composed of experts and members of the *Riksdag* (the Swedish Parliament) with the task of carrying out a survey of and to analyse legislation in Sweden concerning privacy. The committee was later also assigned the task of considering if there, in addition to existing legislation, is need for generally applicable rules to protect privacy. In spring 2007, the committee presented an extensive report – as a result of the first part of the assignment – containing the survey and analysis. The committee describes in relative depth how legislation in different areas of society has developed, what kind of information the government and the *Riksdag* have had to base their decisions on and also how the balance has been struck between the interest of protecting privacy and other interests. The principle of proportionality was the subject of specific analysis. The Committee expresses several points of criticism of a systematic and methodical nature and shows how imperfections in this respect have led to a poorer protection of privacy than necessary. The Committee gives a straight negative answer to the direct question whether the protection of privacy can be considered as satisfactorily regulated. The second and last report of the Committee was presented in January 2008, and in this report the committee gives an analysis of how the constitutional protection of privacy ought to be regulated and what other measures are necessary.

The Commission of Inquiry which in May 2006 was assigned by the Swedish Minister for Justice the task of reviewing national legislation in order to propose amendments required with regard to the adoption

of the *EC Directive on the retention of data processed in connection with the provision of public electronic communication services* presented its report in November 2007. The Data Inspection Board was represented in the inquiry, and during the inquiry work service providers were also consulted. The Ministry of Justice has submitted the report for consideration and the Data Inspection Board is presently studying the proposals of the inquiry. The government will submit a bill to the *Riksdag* later on this year. It is not likely that national implementation of the Directive can take place before 2009.

In last year's Annual Report the proposal for new rules on patient records and healthcare was presented. A completely new act, the Patient Data Act, with a cohesive regulation of personal data within health and medical care services was proposed by the Commission of Inquiry assigned this task. A representative of the Data Inspection Board participated in the work on the proposed new act. The proposal was submitted for consultation and is now under preparation by the government. It is anticipated that the new act will enter into force by 1 July 2008. The inquiry presented its last report, Patient Data and Pharmaceuticals, in the summer of 2007.

In November 2007, the Ministry of Justice presented a report with a proposal for a new act on the processing of personal data by the police in crime combating activities. The proposed new act is meant to replace the Police Data Act of 1992. The proposed new act regulates – with a few exceptions – all processing by the police in their crime combating activities. It will apply to the National Police Board, the police authorities and the Swedish National Economic Crimes Bureau. Specific rules will apply for processing within the Swedish Security Service. The proposed new act also creates possibilities for better co-operation among the crime combating authorities by introducing new rules for disclosure of data. The report has been submitted for consultation and the Data Inspection Board is now considering the proposals. The idea is that the proposals will enter into force as of 1 January 2009.

B. Major case law

A case concerning biometric data in schools was presented in the 9th Annual Report. The case referred to a decision of the Data Inspection Board of 2004 regarding the collection and processing of students' fingerprints for the purpose of checking access to the school canteen. Regardless of the fact that consent was obtained, the decision was that the processing was not adequate or relevant and that such checks could be made in a less privacy-intrusive manner. This view has been upheld in other similar cases. The Data Inspection Board's decisions were appealed to the County Administrative Court which upheld the Board's decisions. The cases were then appealed to the Administrative Court of Appeal in Stockholm which found that such collection and processing meet data protection principles relating to quality and are legitimate without consent. The Data Inspection Board has appealed to the Supreme Administrative Court, and at present three cases are pending there awaiting a review permit.

In June 2007, the Administrative Court of Appeal in Stockholm passed its judgment in the Anti-Piracy Bureau case that had been presented in preceding Annual Reports. This case deals with the issue of whether IP numbers are to be considered as personal data or not. The Anti-Piracy Bureau – a co-operative economic association – had collected scattered pieces of information, in particular IP numbers, in connection with file sharing of copyrighted material on the Internet. The Data Inspection Board stated in its decision that IP numbers were to be considered as personal data and that the processing carried out by the Anti-Piracy Bureau was in breach of the Personal Data Act (PDA), since it implied processing of offences within the meaning of Section 21 of the PDA. Only public authorities may process personal data concerning legal offences involving crime, unless the Board has granted an exemption from that prohibition. The Board ordered, in its decision of June 2005, the Anti-Piracy Bureau to stop the processing. The Anti-Piracy Bureau claimed that the IP numbers could not be considered as personal data since the Bureau did not have access to the personal data identifying the owner of a subscription that uses a certain IP address. The Bureau appealed against the decision. Both the County Administrative Court and the Administrative Court of Appeal upheld the Data Inspection Board's decision.

After the Data Inspection Board's decision in 2005, the Anti-Piracy Bureau applied for an exemption from the

prohibition of Section 21 of the PDA for the purpose of processing IP numbers so that it could report, for instance, to the police and inform Internet service providers of subscribers' copyright infringements. The Data Inspection Board granted an exemption, which was later renewed and the Bureau may process personal data relating to offences until the end of 2008.

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 periodical containing reports, news and commentaries in connection with the Data Inspection Board's fields of interest. Four issues were published during 2007 and the number of subscribers to the printed edition has increased considerably during 2007.

The Data Inspection Board has been assigned by the government the task of contributing to a secure and efficient e-government. As part of this work, we have elaborated *Guidelines for municipalities: Personal data and e-government*. The publication has been distributed to all municipalities in the country. According to the appropriation directions we shall also observe new phenomena and as part of this work we have produced the following reports: *Ubiquitous Computing – a vision which can turn into reality, The Visa Information System (VIS) – the world's largest database with fingerprints* and *The Prüm Treaty gives the police within the* EU *the right to search each other's DNA, fingerprint and vehicle registers*.

A research company has on our behalf investigated the attitude of young people towards the Internet in the report *Young People and Privacy*. We have also published a portrait of our authority - both in Swedish and English – *What on Earth does the Data Inspection Board do?* In this publication we present our activities by letting ten employees talk about their jobs and themselves. Finally we have published a checklist *Electronic keys in housing firms and housing co-operatives*.

With regard to self-regulation, the Data Inspection Board has given its opinion on a new system, ID06, in the construction sector. The aim of the system is twofold; to make it more difficult to use unregistered labour as well as to control – for security reasons – who is actually at the workplace. The Data Inspection Board found that the system complied with the rules of the Personal Data Act, but underlined that the data subjects must be clearly informed. The personal data that is collected may be stored for two years at the most, since the tax authorities might need the data for controls.

The United Kingdom

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

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

Directive 2002/58/EC is transposed into UK law as the Privacy and Electronic Communications Regulations which came into effect on 11 December 2003.

The final transitional period ended on 23 October 2007, meaning that manual records held before 1998 are now subject to the provisions of the Act.

B. Major case law

The Court of Appeal rejected the appeal of David Paul Johnson in the case Johnson v The Medical Defence Union ((2007) EWCA Civ. 262). In their judgment, two of the three judges maintained that the Data Protection Act does not extend to the selection of personal information by a human being, even if that information is then put onto an automated system. It has yet to be seen whether this interpretation will have any ongoing consequences.

C. Major specific issues

In November, Her Majesty's Revenue and Customs (HMRC) admitted that it had lost two computer discs containing the entire child benefit database, with the personal details of twenty-five million individuals. This highlighted the importance of data protection and the limitations on the Commissioner's ability to prevent or penalise such breaches. In December, the Commissioner called on the government to give him greater powers to audit data controllers without their consent and to provide for sanctions for deliberate or reckless breaches of the data protection principles. It is also proposed that a sliding scale will be introduced for notification fees, which would significantly increase the resources available to the Commissioner. The government is expected to consult on these proposed changes in 2008.

During 2007, the ICO conducted a consultation exercise on the new Data Protection Strategy. This strategy will involve focusing the office's resources to make a difference where there is a real risk of harm to individuals. The Commissioner's aim is to make compliance simpler for the vast majority of well-meaning data controllers whilst using his enforcement powers on the minority which pose a real risk to individuals' information rights. The strategy will be launched in March 2008.

In October, Prime Minister Gordon Brown asked Information Commissioner Richard Thomas and Dr Mark Walport of the Wellcome Trust to carry out an independent review into information sharing. Their report will make recommendations on possible changes to the law and policy in this area.

In January 2007, the Commissioner marked the first European Data Protection Day by focusing attention on the risk of identity fraud. The ICO released the results of a survey showing that the majority of people in the UK have either been victims of ID fraud already, or are putting themselves at needless risk. The office produced a short public information film ("The man in the mirror") to raise public awareness of this threat, and issued the "Personal Information Toolkit" – a brief guide to protecting your personal information.

In March, the ICO found eleven banks and financial institutions in breach of the Data Protection Act after media reports that confidential banking details had been disposed of in ordinary bins and plastic sacks. The chief executives of the banks concerned signed written undertakings to improve their security procedures.

In August, the ICO published a paper on the definition of personal data, taking into account the opinion of the Article 29 Working Party.

In October, the ICO published a Framework Code of Practice on Information Sharing. This will help organisations to produce their own protocols governing the exchange of personal information. The ICO also started a consultation on a revised version of the commissioner's CCTV Code of Practice, which was launched in January 2008.

In November 2007, the Commissioner ordered police forces to delete old, minor convictions from the Police National Computer. The Information Tribunal will hear this case in April 2008.

On 11 December, the Commissioner hosted a conference entitled "Surveillance Society: turning debate into action" at the Bridgewater Hall in Manchester. The ICO's Privacy Impact Assessment handbook and associated research was launched at this event. This is the first privacy impact assessment handbook to be produced by a European Data Protection Authority. The ICO is grateful to the Finnish DPA and others for their contributions to this project.

During 2007, the Commissioner provided evidence to seven Parliamentary select committees on ten inquiries (a significant increase on 2006).

- House of Lords select committee on the European Union, sub-committee F (Home Affairs): inquiries into Schengen II, PNR and the Prüm Treaty.
- House of Lords select committee on the constitution: "Inquiry into the impact of surveillance and data collection upon the privacy of citizens and their relationship with the state".
- House of Commons health committee: inquiry into the electronic patient record.
- Home Affairs select committee: inquiry into "The surveillance society?", and evidence submitted on justice and home affairs at a European Union level.
- Culture Media and Sport select committee: the role of the Press Complaints Commission.
- Criminal Justice and Immigration Bill committee: Section 55 of the DPA (the criminal offence of unauthorised access, processing or sale of data).
- Justice committee: the protection of private data.

During 2007, the Commissioner provided responses to 47 consultations (a very significant increase on 2006).

Chapter Three
European Union and Community Activities

3.1. EUROPEAN COMMISSION

Communication from the Commission to the European Parliament and the Council on the follow-up of the Work programme for a better implementation of the Data Protection Directive, Brussels, 7.3.2007[20]

The Commission's First report on its implementation[21] concluded that, although no legislative changes were needed, work had to be done and that there was considerable scope for improvement in implementing the Directive. The report contained a *Work Programme for better implementation of the Data Protection Directive*.

The Communication adopted on 7 March 2007 examined the work conducted under this programme, assessed the present situation, and outlined the prospects for the future as a condition for success in a number of policy areas in the light of Article 8 of the European Charter of Fundamental Rights, recognising an autonomous right to the protection of personal data.

The main conclusions of this Communication were that the Commission does not envisage submitting any legislative proposal to amend the Directive in the immediate future and urges the Member States to ensure proper implementation of national legislation adopted pursuant to the Directive. The activities listed in the Work Programme will be continued, and the involvement of all stakeholders is a solid basis to strive for better implementation of the principles of the Directive; and in order to reap the full benefit of this mandate, Data Protection authorities should also strive to adapt their domestic practice to the common line they decide at the Working Party.

Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), Brussels, 2.5.2007[22]

The purpose of the Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs) is to consider the benefits of PETs, lay down the Commission's objectives in this field to promote these technologies, and set out clear actions to achieve this goal by supporting the development of PETs and their use by data controllers and consumers.

The Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfil data protection rules. The use of PETs would be complementary to the existing legal framework and enforcement mechanisms.

Proposal for a ***Directive of the European Parliament and of the Council amending Directive 2002/22/EC*** *on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, 13.11.2007*[23]

On 13 November 2007, the Commission adopted a Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The primary objective of this proposal was to enhance the protection of personal data and the privacy of individuals in the electronic communications sector, in particular, by strengthening security-related provisions and enforcement mechanisms.

[20] Communication from the Commission to the European Parliament and the Council on the follow-up of the Work programme for a better implementation of the Data Protection Directive, Brussels http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm#follow_up, OJ C 138 of 22.06.2007, p. 17

[21] First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final, of 15.5.2003, OJ C 76 of 25.03.2004, p. 18

[22] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), OJ C 181 of 03.08.2007, p.22: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0228:EN:NOT

[23] COM(2007) 698 final, OJ C 55 of 28.02.2008. p.4 http://europa.eu.int/eur-lex/lex/JOHtml.do?uri=OJ%3AC%3A2008%3A055%3ASOM%3AEN%3AHTML

1st European Data Protection Day: Brussels, 28 January 2007[24]

The Commission welcomed and supported the Council of Europe's initiative to raise the profile of data protection by declaring 28 January 2007 "Data Protection Day", this being the date of signature of the Convention 108 regulating the processing of personal data.

Events took place throughout Member States to inform people about their personal data rights.

Conference on "Public Security, Privacy and Technology", Brussels 20 November 2007[25]

The European Commission organised a Conference on Public Security, Privacy and Technology on 20 November 2007. Technology enables the transfer of data as well as the better control of access to data, and the pinpointing of relevant data, reconciling security and privacy needs. This conference brought together public and private sector representatives.

The conference provided an opportunity to discuss activities encompassing different domains, such as the development of technologies, in particular, privacy enhancing technologies; public-private dialogue on security research and innovation, and how new technologies could be used to increase security.

Protection of personal data under the Treaty of Lisbon

An adapted version of the Charter of Fundamental Rights of the European Union[26] was proclaimed on **12 December 2007 in Strasbourg**. On 13 December 2007, the Treaty of Lisbon[27] was signed by the Heads of State or Government of the 27 Member States in Lisbon. Both introduce important provisions for the protection of personal data:

Article 8 of the EU Charter of Fundamental Rights enshrines everyone's fundamental right to the protection of personal data in a legally binding way.

Article 16 (new) of the Treaty on the Functioning of the European Union provides for a single legal basis for adopting legislative acts relating to the protection of individuals and relating to the free movement of personal data, which will follow the ordinary legislative procedure (co-decision). This applies to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and to the free movement of personal data. The new wording covers in particular police and judicial cooperation in criminal matters at national and EU level, whereby the specific nature of these fields may make specific rules necessary[28].

Article 39 (new) of the Treaty on the European Union provides for a specific legal basis for the protection of personal data in the common foreign and security policy (CFSP) and the rules relating to the free movement of such data. This applies to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 ("Specific provisions on the common foreign and security policy"). This corresponds to the interest of Member States to keep core activities in the diplomatic and defence fields within the intergovernmental realm, and constitutes an exception to the rule of a single legal basis, in line with the principle of primacy of European Community/Union law[29].

2007 PNR Agreement[30]

In Brussels on 23 July 2007 and in Washington on 26 July 2007, an agreement was signed 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 (DHS). This agreement is not

[24] Statement from Vice-President Frattini, on behalf of the European Commission, on the occasion of Data Protection Day (28 January): http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/102&format=HTML&aged=1&language=EN&guiLanguage=en Resolution by the Article 29 Working Party on the 1st European Data Protection Day: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm

[25] For more information on the Conference on "Public Security, Privacy and Technology": http://ec.europa.eu/justice_home/news/events/events_2007_en.htm

[26] OJ C 303 of 14.12.2007, p.1.

[27] OJ C 306 of 17.12.2007, p.1.

[28] Declarations 20 and 21.

[29] Article 40 TEU, as amended by the Treaty of Lisbon.

[30] Council Decision 2007/551/CFSP/JHA of 23 July 2007, OJ L 204 of 4.8.2007, p.16 Agreement between the European Union and the United States of America, OJ L 204 of 4.8.2007, p.18 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:0017:EN:PDF

intended to derogate from or amend the laws of the United States of America or the European Union or its Member States. Its objective is to prevent and combat terrorism and transnational crime effectively as a means of protecting the respective democratic societies and common values of the parties.

Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes (COM(2007) 654 final)[31]

The Commission's Proposal for a Council Framework Decision on the use of Passenger Name Records (PNR) for law enforcement purposes, adopted on 6 November 2007, provides for air carriers making available to the competent authorities of the Member States the PNR data of passengers on international flights, for the purpose of preventing and combating terrorist offences and organised crime. It also provides for the collection and retention of this data by these authorities and the exchange of this data between them.

SWIFT

After the 11 September 2001 terrorist attacks, the U.S. Treasury Department developed the TFTP to identify, track and pursue those who provide financial support for terrorist activity. Under the TFTP, the U.S. Treasury Department has served administrative subpoenas on the Society for Worldwide Interbank Financial Telecommunication (SWIFT). These subpoenas require SWIFT in the U.S. to transfer a limited subset of personal financial data held on its U.S. server to the U.S. Treasury Department where they may be used for counter terrorism purposes regarding suspected individuals or entities.

When these facts became public in 2006, the Belgian Data Protection Authority issued an opinion stating that SWIFT processing activities for the execution of interbank payments were in breach of Belgian data protection law, which implements Directive 95/46/EC on the protection of personal data. The Article 29 Working Party also adopted an opinion in November 2006[32] concluding that SWIFT and the financial institutions which use SWIFT's services had breached Community data protection law as set out in Directive 95/46/EC, including with regard to the transfer of personal data to the United States without ensuring adequate protection and failure to inform data subjects about the way in which their personal data was being processed. During 2007, the Article 29 Working Party continued the follow-up of this case in order to evaluate progress by the different players to address the findings of its opinion of 22 November 2006. The Article 29 Working Party met several times with representatives of SWIFT and banking associations in order to take stock of the steps and initiatives to be adopted to comply with data protection principles.

In parallel with the work carried out by the Article 29 Working Party and national data protection authorities, the Commission and the Council Presidency have worked in order to address the infringement of Community data protection law by SWIFT and financial institutions and resolve the different issues raised.

The Commission has always stressed that in order to solve the different issues raised, it is necessary first that SWIFT and financial institutions comply with the Data Protection Directive, notably by SWIFT taking the necessary steps to respect Belgian DP Law (notify its processing activities to the Belgian DPA) and customers of banks and other financial institutions about the manner in which SWIFT data is processed, the fact they are transferred to the US SWIFT server and that they might be accessed by the US for counterterrorism purposes. Secondly, SWIFT must also ensure that transfers of SWIFT data to its mirror server in the United States for commercial purposes is lawful under the Data Protection Directive. For this purpose, SWIFT joined the US Safe Harbor in June 2007.

Thirdly, the Commission and the Council Presidency have discussed with the US Treasury a set of "Representations" under which the US Treasury unilaterally commits to process EU originating personal data in compliance with EU data protection principles. The Parliament (LIBE

[31] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes (COM(2007) 654 final), OJ C55/4: http://europa.eu.int/eur-lex/lex/JOHtml.do?uri=OJ%3AC%3A2008%3A055%3ASOM%3AEN%3AHTML

[32] Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128). http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm

Committee) and Council (COREPER) have been kept regularly informed of these discussions, as well as the Article 29 Working Party. On 28 June 2008, the US Treasury informed the Council Presidency and the Commission on the "Representations of the US Department of the Treasury with regard to the handling, use and dissemination of data obtained under the Terrorist Financing Tracking Program" (TFTP).[33]

3.2. EUROPEAN COURT OF JUSTICE

Judgment of the Court of First Instance of 8 November 2007 - Bavarian Lager v Commission (Case T-194/04)[34]

The Third Chamber of the Court of First Instance of the European Communities annulled a Commission Decision of 18 March 2004 rejecting an application for access to the full minutes of a meeting. The Court of First Instance held that a request to the Commission of the European Communities for access to personal data contained in a Commission document could only be refused on the grounds of the privacy and integrity of the persons if such privacy and integrity were capable of being actually and specifically undermined by disclosure, and the applicant did not have to prove that disclosure was necessary. The Commission has appealed.

3.3. EUROPEAN DATA PROTECTION SUPERVISOR

Introduction

The main activities of the European Data Protection Supervisor, as laid down in Regulation 45/2001[35], are to:

- supervise the EU-administration's processing of personal data, making sure that the rights and freedoms of individuals whose data are processed are not violated (supervision);
- give advice on proposals for new EU legislation with an impact on data protection (consultation);
- cooperate with other data protection authorities to ensure a high and consistent level of data protection throughout Europe (cooperation).

In 2007, substantial progress was achieved in the area of supervision. The emphasis on measuring results has led to investments in meeting data protection requirements in most Community institutions and bodies. There is reason for some satisfaction, but continued efforts are needed to reach full compliance.

In the field of consultation, much emphasis has been placed on the need for a consistent and effective framework for data protection, both in the first and in the third pillars, but not always with satisfactory results. However, an increasing variety of policy areas now benefits from the consultative activities of the EDPS.

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

Supervision

The supervisory tasks, led by the Assistant Supervisor, range from giving advice and assisting Data Protection Officers (DPOs), through prior checking risky processing operations, to conducting inquiries and handling complaints, etc. This work also consists of elaborating background and position papers, and of supervising the central unit of Eurodac.

In 2007, **prior checking** continued to be a major activity in the EDPS supervision task. The deadline of spring 2007 for receipt of notifications to be prior checked by the EDPS – *ex post* cases – was fixed to trigger Community institutions and bodies to increase their efforts towards a complete fulfilment of their notification obligation.

[33] OJ C 166 of 20.7.2007, p. 17.

[34] OJ C 315 of 22.12.2007, p.33.

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

Overall, the EDPS prior-check exercise during 2007 shows that the **"spring 2007" deadline** gave rise to a tremendous increase of notifications from many data protection officers, especially during the first semester of the year. However, there is still much to improve regarding the time frame used by institutions and agencies to answer the requests for further information from the EDPS.

In 2008, efforts will therefore mainly concentrate on the following points:

- institutions should finalise their *ex post* notification process and agencies should make a substantive step towards the same goal in 2008;
- the follow-up of recommendations will continue to take place systematically through information from the controller, and will be combined with on-the-spot inspections.

65 **complaints** were received in 2007. Cases declared admissible related in particular to the collection of excessive data relating to visitors, access to data, forwarding and copying of e-mails, requirement of credit card details, processing of sensitive data, right of rectification and obligation to provide information.

A number of **inquiries** were conducted in different areas during 2007. Among them, two required special attention from the EDPS, namely the OLAF Security Audit and the role of the European Central Bank (ECB) in the SWIFT[36] case.

The EDPS also continued to provide advice on **administrative measures** envisaged by Community institutions and bodies in relation to the processing of personal data. A variety of challenging issues was raised, including the setting up of conservation periods for certain categories of files, Internet policy papers, investigation procedures against fraud and corruption, exchange of information, implementing rules concerning data protection and applicability of national data protection law.

The EDPS continued to work on his **video-surveillance guidelines** to provide practical guidance to institutions and bodies on compliance with data protection rules when using video-surveillance systems.

Joint work on the shared supervision of **Eurodac** continued together with the national data protection authorities throughout 2007. Following the launch of an in-depth security audit in September 2006, a final report of the audit was presented in November 2007. The main conclusion was that security measures initially implemented with respect to Eurodac and the way in which they have been maintained during the first four years of activity have provided a fair level of protection to date. However, some parts of the systems and the organisational security present certain weaknesses which will have to be addressed.

Consultation

In 2007, the activities of the EDPS took place in the context of different developments having as a common denominator the fact that they all contributed to the emergence of a "**Surveillance Society**". Such developments include new instruments for law enforcement to collect and process personal information, the increased use of biometrics and RFID, as well as the growing importance of worldwide data flows.

The EDPS issued **12 opinions** on proposed EU legislation in 2007. In the area of freedom, security and justice, a major concern was the adoption of new proposals facilitating the storage by and exchange of information between law enforcement authorities, without a proper assessment of the effectiveness of existing legal instruments. This issue was of particular relevance in relation to the transposition of the Prüm-Treaty to EU level and to the European Passenger Name Record system.

Another issue that played a central role in the opinions of the EDPS related to the third pillar was the lack of a comprehensive legal framework for data protection.

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

[36] Society for Worldwide Interbank Financial Telecommunication.

data is transferred between the authorities of different Member States.

The exchange of information with third countries for law enforcement purposes was a separate issue, addressed in different EDPS opinions.

In a more general context, two opinions were issued with regard to key Commission communications on the **future framework for data protection**. In his Opinion on the Implementation of the Data Protection Directive[37], the EDPS identified various perspectives of a changing context, one of which being the interaction with technology. New technological developments have a clear impact on the requirements for an effective legal framework for data protection. One crucial feature of these technological developments is **Radio Frequency Identification**, which was the subject of a separate EDPS Opinion.

In December 2007, the **Inventory 2008** (the second yearly inventory) was published on the EDPS website. It follows the main lines as set out in the Inventory 2007. The Annex of the Inventory shows that the scope of activity of the EDPS now covers a wide range of policy areas.

Five **perspectives for future change**, which will serve as the agenda for future activities of the EDPS, have been identified in his Opinion on the Communication on the Implementation of the Data Protection Directive, namely:

- interaction with technology;
- impact of the Lisbon Treaty;
- law enforcement;
- global privacy and jurisdiction; and
- full implementation of the Directive.

Cooperation

The main forum for cooperation between the data protection authorities in Europe is the **Article 29 Working Party**. The EDPS participates in the activities of the Working Party, which plays a crucial role in the uniform application and interpretation of the general principles of Directive 95/46.

The EDPS welcomes the opinions of the Working Party, which have been consistent with his own opinions and to which he actively contributed. Examples of good synergies between the opinions of the Working Party and the EDPS during 2007 were in the fields of common consular instructions on visas for diplomatic missions and consular posts in relation to the introductions of biometrics, as well as airline passenger data transfers to the US and the use of passenger name record for law enforcement purposes.

The EDPS and the Working Party have also closely collaborated in the analysis of two large systems in the first pillar, namely the consumer protection cooperation system and the internal market information system.

One of the most important cooperative tasks of the EDPS relates to **Eurodac**, where the responsibilities for data protection supervision are shared between the national data protection authorities and the EDPS. In July 2007, the Eurodac Supervision Coordination Group – composed of national data protection authorities and the EDPS – issued a report on their first coordinated inspection of Eurodac. The Group did not find indications of abuse of the Eurodac system. However, some aspects, such as information to the people concerned, need to be improved.

The EDPS strives to ensure a high and consistent level of data protection in the works of the Joint Supervisory Bodies for Schengen, Europol, Eurojust and the Customs Information System. In 2007, attention focused on two main subjects: the Commission proposal for a framework decision on data protection in the third pillar and the exchange of law enforcement information in accordance with the principle of availability.

The EDPS also took part in the **European and International Conferences** on data protection and privacy. The latter, which took place in Montreal in September 2007, focused on the many issues data protection and privacy commissioners are dealing with, such as public safety, globalisation, law and technology, "ubiquitous computing" and "body as data". The

[37] Opinion of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, p. 1.

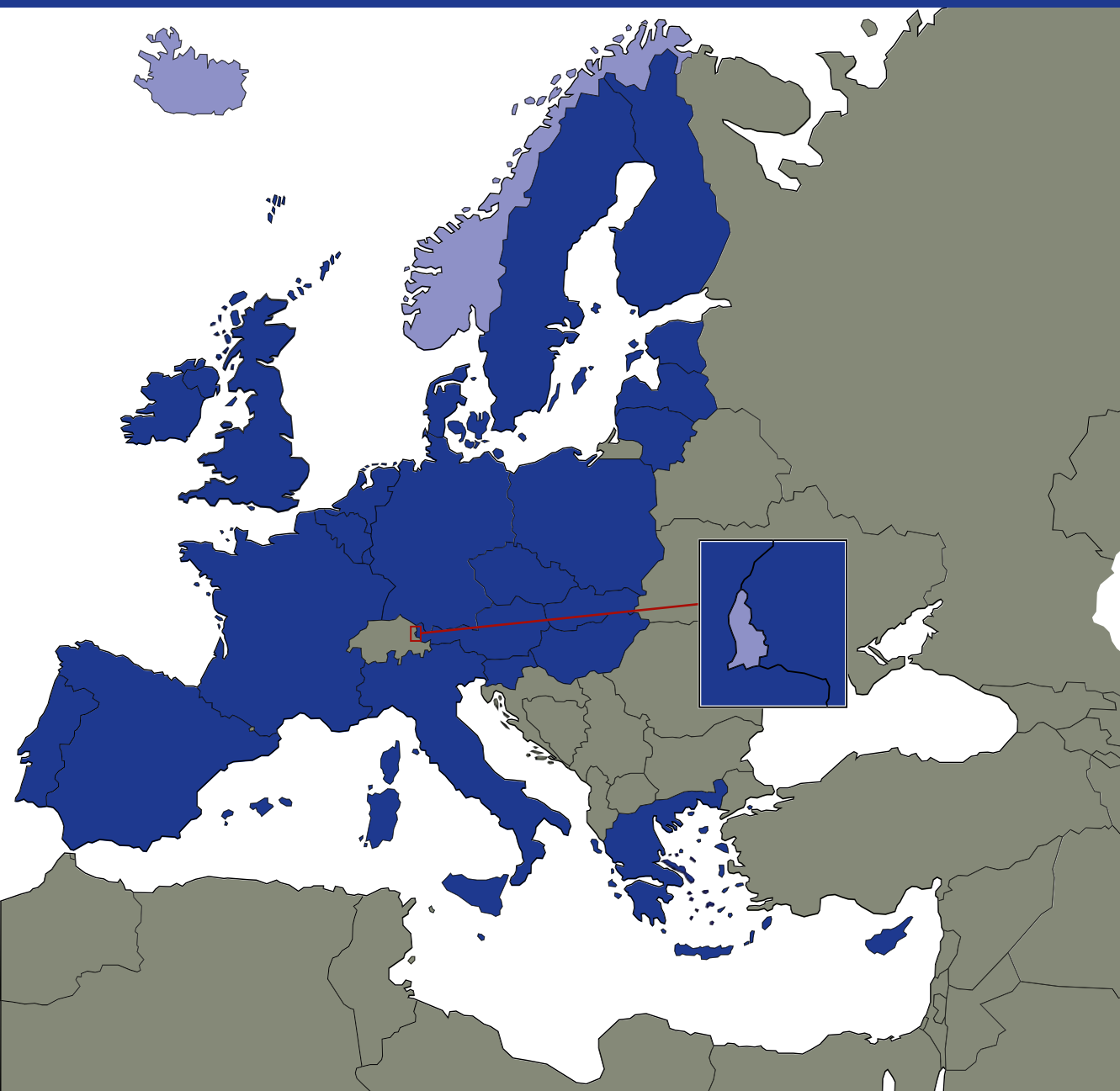
EDPS chaired a closed session for commissioners on the London initiative and contributed to a workshop on globalisation.

Communication

Increasing the EDPS' visibility on the EU political map was a clear focus of the EDPS' communication activities during his initial years of activity. Three years after the start of work, we can now see positive results in his communication endeavours. One example of this is the selection of the Supervisor as one of the European Voices' 50 nominees for the 2007 European of the Year Award.

As one of the main architects of the "London Initiative" designed to make communication on data protection and data protection itself more effective, the EDPS followed this up in February 2007 by actively participating in the communication workshop hosted by the French data protection authority (CNIL). One significant result was the creation of a network of communication officers that data protection authorities will be able to use to exchange best practices and to carry out specific projects.

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 legal acts concerning data protection were passed regarding Directive 95/46/EC (but none, however, regarding Directive 2002/58/EC). These are the most important ones:

1. Act No 36/2007 Changing Act No 66/1985 on the National Archives. According to Act No 36/2007, a special section within the National Archives shall keep all documents regarding the national security of Iceland in the years 1945–1991. The act was passed when there had been widespread discussions about telephone tapping which occurred in the Cold War years. This telephone tapping was, e.g. directed at individuals who were influential in the workers' movement and the Socialist Party. The aim of the act was to make documents about these events, e.g. court orders – and about national security in those years in general – available to the public and the individuals in question, i.e. those who are mentioned in these documents. In spite of that, personal data of a sensitive nature regarding persons other than those claiming access will be erased from copies of documents. However, if an individual, on whom such data is kept, gives his consent to its disclosure, the data is made available to the public.

2. Act No 40/2007 on Health Services. According to Art. 20 of the Act, the National Hospital shall, *inter alia*, operate a blood bank. However, there are no further provisions on this blood bank, e.g. on the protection of personal data. In the older Act on Health Services, No 97/1990, there were, on the contrary, more articulate provisions, amongst them that the Data Protection Authority had the role of supervising the processing of personal data within blood banks. The lack of provisions in this respect was criticised in the DPA's opinion on the bill, which later approved as Act No 40/2007. However, no changes were made to the bill in accordance with this criticism.

3. Act No 41/2007 on the National Directorate of Health. The Act contains provisions on the processing of personal data, the most important of which regard registers kept by the National Directorate of Health. According to Art. 8 of the Act, patients are not asked for their consent before their data is entered into these registers, i.e. registers on births, heart and vein diseases, nervous diseases, cancer, accidents, admittance to health institutions, communication between clinics, and communication between independently practicing health professionals.

The National Director of Health (the head of the Directorate) is responsible for these registers. However, not all of them are kept within the National Directorate of Health. The register on cancer is, e.g. kept by the Icelandic Cancer Society. Personal identity markers in the registers must be encoded. The processing of personal data must be carried out in accordance with the Data Protection Act, No 77/2000, and the security of data must fulfil the DPA's requirements. All use of data for scientific research must be based on permits issued by the DPA.

Furthermore, according to the Medicinal Products Act, No 93/1994, cf. Act No 89/2003, the National Directorate of Health keeps a medicinal database with data on all prescriptions from the last three years (this is also mentioned in the chapter on Iceland in the Annual Report for 2002 and 2003). Personal identity markers are encoded, but it is possible to decode them. There is now a bill in Parliament on prolonging the retention period to 30 years. The DPA is strongly opposed to this and has issued opinions in that regard.

4. Act No 163/2007 on the Statistical Office of Iceland. According to Art. 5-8, the Statistical Office collects data – including personal data – for statistical research. The Statistical Office is, according to Art. 9. of the Act, allowed to link its registers and registers from other parties by using personal identity numbers or other identification markers.

There are also provisions in the Act regarding the protection of personal data, e.g. that employees of the Statistical Office are under an obligation of secrecy, cf. Art. 11, and that confidential data shall be deleted after being used unless it can be of further use for statistical research, in which case personal identity markers shall be hidden or deleted, cf. Art. 12. Also according to Art. 12, the Statistical Office shall pass rules on the security and retention of confidential data, e.g. on retention

and destruction of paper documents, whether and when computerised data shall be deleted and personal identity markers in such data hidden or encoded.

Art. 13 contains a provision stating that the Statistical Office can give third parties access to sensitive personal data for research purposes, given that they will return the data or destroy personal identity markers when the research project in question has been completed. In an opinion on the bill, which later approved as Act No 163/2007, the DPA suggested that it should be added that there should always be a certain time limit for third parties' retention of data and, also, that if the researcher intended to retain data for a longer period, he should ask for the Statistical Office's consent. This suggestion was adhered to.

However, Parliament rejected the DPA's suggestion that there should be a provision in the Act on the encoding of data when linking registers in accordance with the aforementioned provision of Art. 9.

B. Major case law

On 6 December 2007, the Supreme Court of Iceland gave judgement regarding the DPA's Decision of 27 February 2006. The case was filed by a doctor who, 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 DPA 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 in a judgement given on 21 December 2006 (this judgement is mentioned in the chapter on Iceland in the Annual Report for 2006).

However, the Supreme Court nullified the DPA's decision. In that regard, the court pointed out that the individual in question had given his advocate written permission to access his health records. The advocate had given a copy of the permission to the doctor. On these grounds, the court considered the doctor to have acted in good faith when he accessed the individual's health record. This means, in other words, that the court was of the view that the doctor had reason to believe that the individual had consented to this access even though there was no written permission in that regard from this individual to the doctor himself.

C. Major specific issues

The most major cases handled by the DPA in 2007 are as follows:

On 19 February 2007, the DPA decided on the lawfulness and security of access to electronic patient records in the National Hospital. The hospital had given certain employees, including all doctors, very wide access rights, i.e. to all electronic health record information on all patients – with the exception of certain categories of data, e.g. data regarding psychological diseases which were kept in a special unit. According to the hospital, the wide access was necessary because the employees in question treated patients in all departments of the hospital and gave advice regarding treatment in all departments. The DPA did not reconsider this evaluation. However, the DPA decided that strict security measures should be implemented, e.g. that employees should state their reason for accessing a health record (e.g. by ticking a box), that all access should be logged, and that the logs should be reviewed regularly.

On 26 June 2007, the DPA decided that the National Directorate of Health was not allowed to give researchers access to sensitive data, amongst them data on abortions. The researchers had requested access to data on women who had taken part in a research project regarding contraception. According to the information given to the women, data collected on them would be deleted when the project was completed. However, long after the completion of this previous project, more data was now to be collected on the women without asking for their consent. The DPA considered this to be in breach of the Data Protection Act, No 77/2000, and because of that, the authority came to the aforementioned conclusion. In the wake of this, the researcher deleted all personal data which had been collected in the course of the previous project.

On 6 October 2007, the DPA decided on the collection of data by an aluminium factory in the community of Hafnarfjördur regarding the opinions of the community's inhabitants to a proposed enlargement of the factory.

The inhabitants were telephoned and asked for their opinion. Then, data on their opinions was put into an electronic database without informing them of this. The DPA came to the conclusion that this was in breach of the Data Protection Act.

On 26 November 2007, the DPA decided on the use of fingerprints in a primary school canteen. The fingerprints were used as a means of identification of those entitled to school meals. The equipment made use of templates for comparison with students' fingerprints. Those templates could not be used to restore fingerprints. Parents of children consented to this processing, and they could choose to have so-called meal cards issued to their children instead. The DPA came to the conclusion that the processing was not in breach of the Data Protection Act.

On 26 November 2007, the DPA decided on whether permission should be given on linking together genetic data in different research projects conducted by the genetic research company deCode. The data would regard 85,000 individuals who had taken part in 66 projects. These individuals had consented to their data being kept for use in a certain project, but also for use in further projects given that the DPA and the National Bioethics Committee granted their permission. In the light of this, deCode did not intend to ask for the data subjects' consent to the linking of data. If it would come to light that they had a genotype often occurring in individuals in another project, their data would be added to that project. Personal identity markers would be encoded, but it would be possible to decode them. The DPA considered that this processing was too vast to fall under the individuals' consent to the use of data in further research. Furthermore, the DPA considered that it was not empowered to allow this processing. Therefore, the DPA declined issuing a permit.

On 10 December 2007, the DPA decided on the lawfulness and security of the two biobanks of the Icelandic Cancer Society. According to the Icelandic Act on biobanks, No 110/2000, biosamples in biobanks must always be kept apart from personal identity markers. This, however, was not the case with one of the biobanks of the Society, and the DPA ordered it to change this before 1 September 2008. This biobank is used for treatment purposes, and now, a bill has been prepared stating that in such cases, it is not necessary to keep biosamples in a biobank apart from personal identity markers.

Liechtenstein

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

One of the tasks of the Data Protection Commissioner (DSB) is to adopt a position on parliamentary bills and regulations that are relevant to data protection, and verify that they comply with the provision of Directive 95/46/EC. In 2007, DSB issued a position paper on over 20 parliamentary bills. There follows a brief presentation of some of them:

With regard to the position papers on the discussion stage of the amendment of the *Law on the Recognition of University Diplomas and Vocational Qualifications*, the *Medical Practitioners Act*, the *Veterinary Medicine Act*, the *Law on the Legal Profession, Trustees and Patent Lawyers* as well as on the *Law on Engineers and Architects Working in the Construction Industry*, it was mainly the introduction of the Internal Market Information System (IMI) which was relevant to data protection issues. The importance of uniform rules for the various professional groups was stressed in the position papers. Fundamentally, it was emphasised that it was important to keep as close as possible in the various legal texts to the text of Article 56 para. 2 of the Vocational Qualifications Directive and the wide-ranging position paper of the Article 29 Data Protection Working Party on the data protection aspects of the IMI (WP 140). Not all of the amendments of the laws related to the IMI had been adopted at the end of the reporting year 2007.

The Reuse of Public Sector Information Directive 2003/98/EC was implemented into national law by the enactment of a *Law on Reuse of Information by the Public Sector (Reuse of Information Act)*. In its Position Paper, the DSB referred to Position Paper 7/2003 of the Article 29 Data Protection Working Party Group on the Reuse of Information by the Public Sector and Protection of Personal Data of 12 December 2003 (WP 83). On the other hand, the DSB urged simultaneous amendment of the Data Protection Act, Art. 17 para. 2, subpara. f and Art. 23 para.1 subpara. c. Unlike some other national data protection acts within Europe, under the Liechtenstein legal text, personal data can only be used if the person concerned has made the data generally available himself/herself. However, in this respect the DSB is endeavouring to achieve a more liberal approach. For this reason, the DSB has proposed an amendment to the Data Protection Act to the effect that if the personal data is generally accessible to the public, this will suffice as legal grounds for use (e.g. the telephone directory). This would allow a more liberal approach, which would be more sensible and desirable, including from the perspective of the new Reuse of Information Act. The right to object under Art. 16 para. 3 of the Data Protection Act remains unaffected by this.

During the reporting year, the amendment of the *Unfair Competition Act (UWG) was pending,* which is to implement the provisions of European Directive 2005/29/EC on unfair business practices, which aims in particular to simplify cross-border trade. New provisions to be introduced in Liechtenstein will include rules that not only faxes and e-mails, but also persistent and unsolicited advertising over the telephone are considered as aggressive business practices, which are deemed unfair when they are persistent. This gave rise to a different judicial assessment of unwanted advertising to that in the Liechtenstein Communications Act, depending on the medium used: under the prevailing Liechtenstein Communications Act, advertising that is sent without the prior consent of the recipient by fax/e-mail, is in principle banned from the very first sending.[38] Unsolicited advertising by telephone, on the other hand, is not covered by the Communications Act. The revision of the Unfair Competition Act does not ban unsolicited telephone advertising from the very first call, and will only result in consequences under the (criminal) law when it is "persistent" as defined by the new Unfair Competition Act. As a result, a legal distinction will be introduced in Liechtenstein between unwanted advertising by telephone as opposed to that by fax or e-mail. In its position paper on the revision of the Unfair Practices Act, the DSB stated that it would be in the interest of consumers to point out this discrepancy, and to promote equal treatment of all media in the interests of effective consumer protection.

[38] Art. 50 Communications Act (KomG).

Furthermore, the amendment of the *Police Act*, which came into effect in 2007, was also of particular relevance to data protection. In the context of police investigative powers, miscellaneous new legal bases were created: under certain circumstances, the collection and processing of biometric data is allowed; and the use of image and sound recordings at mass events or places accessible to the general public is only possible under certain conditions. The authorisation in principle of video surveillance by the national police has been the first and only legal measure in Liechstenstein to date to allow video surveillance in public places, and for that reason alone is of decisive importance to data protection. Furthermore, many arrangements for (international) administrative assistance as well as the legal basis for an electronic information system have been created. This information system is not entirely unproblematic from the data protection viewpoint, since it is intended to enable the interconnection of various databases. In addition, a completely new indirect right to demand information has been introduced. If the state security services or authorities carrying out investigations to prevent a crime are involved, the person concerned can make a request, not personally but via the Data Protection Commissioner, to establish whether data about him/her is being processed. Up to the end of 2007, no one had availed themselves of this indirect right to request information.

The amendment of the *Law on Acquisition and Loss of National Citizenship* as well as the *creation of a legal basis for the central register of persons of the Liechtenstein national administration (ZPV)* – a legislative proposal which has been topical for several years due to the data protection issue which could not be adopted in 2007[39] - are of national significance.

In the context of the amendment of the *Banking Act*, ultimately obligations that were relevant to data protection and related to cooperation with the authorities concerning customers, as well as a general obligation to provide information about bank customers were introduced. It is worth mentioning that this information obligation is not only about existing customers, but also, following the example of Directives 2004/39/EC and 2006/73/EC about potential customers.

In this regard, it is also worth mentioning *EU Regulation 1781/2006* (on information on the payer accompanying transfers of funds), which had not yet entered into force in Liechtenstein in 2007. Since it was already applicable in the EU in 2007, the regulation already has some effect for Liechtenstein, notably for cross-border funds transfers between a Liechtenstein bank and a bank in the EU area. A number of Liechtenstein banks saw this as a reason to inform their customers about the effects of this regulation in the reporting year, although it has not yet been implemented into Liechtenstein law.

B. Major case law

The Liechtenstein State Court, as the Constitutional Court, handed down a landmark ruling on (international) administrative assistance and banking secrecy[40]. According to the judgement, secrecy about bank customers is a constitutional issue even if it only concerns the application of laws. This should protect the financial aspects of secrecy and privacy of a legal subject within the scope of the law. This protection is guaranteed by the right to personal freedom enshrined in Article 32 of Liechtenstein's national constitution.

Banking secrecy will not be infringed upon if the regulatory authorities observe the principles of speciality, confidentiality and the "arm's length" principle and proportionality in a request for administrative assistance. Administrative and judicial assistance are not always easy to distinguish from one another. The administrative assistance procedure cannot circumvent judicial assistance, if the administrative assistance complies with these principles. Since, in addition to an initial suspicion, further elements must be provided, which show a sufficiently well founded suspicion for the presence of criminally relevant conduct, "fishing expeditions", i.e. administrative assistance procedures as an abusive cover for finding evidence, are not possible or allowed.

C. Major specific issues

With regard to access by the US authorities to data on international financial transactions (SWIFT transactions),

[39] See 9th Annual Report of the Article 29 Working Party on Data Protection, S. 128.

[40] Judgement of the State Court of 6 February 2006, StGH 2005/50, but which was only published in 2007 in: Liechtensteinische Juristenzeitung, 2007, LES 4/07, p. 396 onward.

the banks complied with the call from the Data Protection Commissioner and amended their General Terms and Conditions of Business. Now it should be pointed out that in cases of settlement via international channels, the transaction data goes abroad. In this case, this data is no longer covered by Liechtenstein law, and it is no longer guaranteed that the level of protection of the data corresponds to that which prevails in Liechtenstein. Finally, it should be borne in mind that foreign legal and regulatory provisions oblige the banks and system operators concerned to divulge this data about third parties.

Furthermore, advice was given on a project on Integrated Case Management[41]. In the view of the Data Protection Commissioner, this was a matter of incorporating the necessary data protection declarations, confidentiality and non-disclosure agreements.

The rising demand from authorities to use video surveillance gave rise to sometimes controversial discussions in the course of 2007. A case of video surveillance of public areas by an authority was submitted to the Data Protection Commission for a ruling. The case was not decided by the end of 2007.

In general, there has been a slight increase in questions[42] as well as hits on the home page[43]. This certainly reflects growing awareness about data protection among the population. The Internet site enables interested parties to find out about topical themes and read guides to the interpretation and applicability of the Data Protection Act, the so-called guidelines. "Guidelines on Video Surveillance by the Authorities" and "Guidelines on Dealing with Unsolicited Advertising, particularly Spam" were published in 2007 for the first time.

[41] Integrated Case Management is intended to make it easier for a worker who has been unfit for work for longer than 6 weeks to return to work. A new regulation provides, inter alia, that the employer must notify the health insurance fund after no more than 6 weeks of sick leave, so that they can appoint a case manager. This Case Manager contacts the employee and inquires whether he/she can do anything to facilitate a return to work. The worker can accept or decline the offer.

[42] In the reporting year 2007, a total of 338 questions were registered and handled.

[43] In the reporting year 2007, the number of hits on the SDS home page was 54,679.

Norway

A. Implementation of Directive 95/46/EC Significant changes to privacy or data protection law

Note to report

Significant changes to other laws affecting privacy or data protection
Amendments to the act relating to the implementation of penalties and the General Civil Penal Code – introduction of the duty to inform, requirements regarding previous good conduct, and notification to the aggrieved party etc.

The amendment entails an extended duty to inform the aggrieved party or the survivors of the aggrieved party, which means that it also applies during pre-release day leave and when punishment is served outside prison. The notification shall *inter alia* comprise the time and conditions of serving the punishment if the conditions directly affect the aggrieved party or his/her survivors. These conditions may relate to place of residence, whether the convicted person is to be prevented from contacting certain persons, and if the convicted person changes his/her address.

When the amendments were on an ordinary round of consultations, the Data Inspectorate stated that, the proposed amendments are based unilaterally on the aggrieved party's standpoint, and that the consequences for the convicted person would have to be examined further. The Data Inspectorate also required the information provided to be kept to a minimum, and no reason could be found as to why the aggrieved party needed at all times to know the convicted person's address, including during the probation period. It should be sufficient to know that the convicted person is no longer in prison. The Data Inspectorate also pointed out that Norwegian Correctional Services are under a general obligation to inform the convicted person of this duty to inform.

At the same time, new and stricter rules were adopted relating to prisoners' use of electronic communications in prison. The Data Inspectorate argued that it was unclear whether the proposed tightening up was in fact necessary and claims that the right to electronic communication in our present technological society must be likened to traditional post and telephone services if this is possible in the light of the correctional services' available resources.

Amendments to the rules on publication of lists of assessed taxes
In 2004, the rules governing the publication of lists of assessed taxes were tightened up, making the lists available for individual searches for only three weeks after publication. The lists of assessed taxes were then posted electronically on the tax authority's website and provided in hard copy at the tax offices. In 2007, an amendment to the law again gave media access to complete lists of assessed taxes on CD-ROM. The Government stated that its reasons included a wish to strengthen the critical debate on the tax system.

The Data Inspectorate deems the amendment to the law as unfortunate. The question relating to the publication of lists of assessed taxes has been of concern to the Data Inspectorate for several years. It is the Data Inspectorate's opinion that it contravenes key principles relating to the protection of personal data when information that individual Norwegian citizens are obliged to submit is used for entertainment, is made the subject of searches and can be sold via mobile telephones in the form of SMS services or similar. It is also questionable that the lists of assessed taxes are published before the time limit for appeals against the tax assessment has expired.

New rules on "grooming"
New rules that make it a criminal offence to meet a child with the intention of committing sexual offences have been introduced. The Data Inspectorate stated that it is commendable that politicians are attempting to find means of preventing sexual abuse of children. However, it was pointed out that, from a personal data protection perspective, exactly which measures are attached to the penal provision represents an interesting question, i.e. which investigative methods the police are to have at their disposal in order to achieve the provision's objective.

B. Major case law

None to report.

C. Major specific issues

Supervisory inspection of the prison service

The Data Inspectorate has strongly criticised the Ministry of Justice and Police following an inspection of the treatment of sensitive personal data taking place in the prison service. The serious breaches of the law that have been revealed show that the right of privacy of more than 30,000 former prisoners and their next of kin has not been observed.

For several years, the Data Inspectorate has received complaints from inmates in Norwegian prisons relating to the handling of personal data in the prisons. Most of the complaints have concerned the lack of proper protection of information about the prisoners and their next of kin.

After the inspection, the Data Inspectorate concluded that there is an unofficial and open personal register at Ila Prison ("inmates by number"). The register contains very sensitive personal data. Furthermore, the use of personal data in the applied professional system lacks a legal basis. The basic rights of the registered persons under the Personal Data Act in respect of the right of access, correction and deletion are not being followed.

Extensive leaks from the telecom companies – formal complaint

During the period from about 28 July to about 7 August 2007 the websites of several telecom companies were used to harvest personal data information. The harvesting of personal data started with a list of possible personal ID numbers stored by a data program. These were subsequently compared with an official website in order to weed out numbers that were not in use. Thereafter the numbers were used to search and find individual persons' names and addresses via the telecom operators' websites. Few of the affected persons had any connection to the telecom enterprises and very many were upset and surprised that this affected them of all people.

The Data Inspectorate holds that the most serious breaches clearly concern the inadequate safeguarding of information, the lack of providing additional information, and the fact that several enterprises did not bother to notify the victims of the incident. The failure to notify affected persons is proof of a lack of respect for individual persons' right of privacy.

The Data Inspectorate decided to make a formal complaint on the breach of the provisions of the Personal Data Protection Act relating to the safeguarding of information and on the provision governing the duty to notify the Data Inspectorate. Several of the registered persons also made formal complaints. Initially, the formal complaints were dropped by the prosecuting authority but are now being reconsidered.

New Freedom of Information Act and regulations

A new Freedom of Information Act has been adopted and is proposed to come into effect on 1 July 2008. The proposed regulations related to the new Freedom of Information Act, which have been undergoing a round of consultations, instruct a number of public bodies and departments to make their electronic post records available on the internet. It also suggests that documents should be made public as far as possible. This publication of large amounts of information about individuals is of concern to the Data Inspectorate. A mass harvesting of personal information is capable of providing extensive profiles of individual persons. This information may be useful for marketing purposes but could also be used for ID theft. Those wishing to steal an identity are able to obtain a virtually complete overview of individual persons' actions and preferences.

The Data Inspectorate has seen a number of examples of municipalities having published personal information that should not have been available on the Internet. Some of the documents have contained information about date of birth and ID numbers, others concern individuals in a crisis situation who have sought help from the municipality, while others have been job applications complete with scanned diplomas and references. When mistakes happen they can have dire consequences for the person concerned. Departments and municipalities finding that confidential personal information is published often explain this as human error. The Data Inspectorate is of the opinion that repeated "accidents" indicate system failure at the organisation.

Working life – access to employee's e-mails – formal complaints

In 2005, the Data Inspectorate made two formal complaints against two enterprises for breach of the Personal Data Act's provisions relating to the duty to inform in relation to access to employees' e-mails. In 2006, the prosecuting authority

dropped both cases. The Data Inspectorate appealed against both discontinuations but they were maintained by the Director General of Public Prosecutions. However, the Director General of Public Prosecutions requested that the Public Prosecutor should investigate further to discover whether employees in one of the enterprises had withheld information from the Data Inspectorate. In October 2007 this case was also discontinued.

In 2006, the Data Inspectorate filed a formal complaint against a publisher for breach of the Personal Data Act. The background to the case was that the manager of the publishing company via a "surveillance account" automatically made blind copies of ingoing e-mail correspondence to the head of the publisher's office in Sweden. The employee's personal e-mail account was protected by means of a user name and a personal password. Thereafter, the publisher accessed the employee's ingoing e-mails through the "surveillance account". The employee who downloaded and opened his ingoing e-mails was not informed about the downloading of the e-mails, the accessing of them, the purpose of the action or any disclosure of the information.

Both the publishing company and the publisher were in 2007 charged with breaching their duty to inform and both were issued with fines, which they accepted.

Road toll chips – AutoPASS

In spring 2007, the Data Inspectorate received information that all crossings through the road toll stations were routinely photographed. This information did not correspond to the official specification of requirements relating to AutoPASS or to the information previously received by the Data Inspectorate on the subject from the Directorate of Public Roads. Consequently, the Directorate of Public Roads was asked to confirm/refute that all crossings through the road toll stations in Norway are photographed. On the basis of the reply from the Directorate of Public Roads, the Data Inspectorate found that photographs are taken of all vehicles that pass through the road toll stations. However, the photos are only forwarded in the system if the passing is invalid or when making random checks. Another restraining factor is the fact that the internal memory of the camera is limited and that the photographs that are not forwarded are therefore overwritten relatively quickly. The Data Inspectorate finds it regrettable that neither the general public nor the Data Inspectorate has been informed of the matter at an earlier stage. It is assumed that the system will be improved.

The 100 most recent crossings are stored in the AutoPASS chip

In the beginning of the notification year, the Data Inspectorate revealed that the 100 most recent crossings through the road toll stations made by AutoPASS users were recorded in their AutoPASS chip. Furthermore, other passing points were also recorded. The Data Inspectorate also reacted to the fact that this personal information was stored on remote-readable chips, completely without confidentiality protection. The most serious contravention is nonetheless that the approximately one million users of AutoPASS have not been actively informed that the chip on their windscreen also has storage capacity for information on time and place of the one hundred most recent crossings.

New health research law

In summer 2007, a proposal for a new law on medical and health-related research was presented to the Storting. In the opinion of the Data Inspectorate, the proposal contains several unclear issues, including with regard to the scope of the Data Inspectorate's authority under the law. The formal key rule of the proposal is that research on health information must be based on consent from the person the information pertains to.

However, the draft legislation contains such a large number of opportunities to disregard consent that the *de facto* and practical key rule of the need for consent could easily become that consent is unnecessary.

The draft legislation also introduces a new legal concept, notably "general consent". This form of consent extends further than what is at present accepted and can be compared with accepting an agreement without being allowed to read the terms and conditions. The fact that this is defined as "consent" according to the draft of the Health Research Act is unfortunate in the opinion of the Data Inspectorate. We are in danger of undermining the individual's basic right to information and self-determination, which could become a strain on the trust that is essential between society and the doctor. The Data Inspectorate has requested the Storting to consider the positive and negative effects of the Act more closely before adopting it.

Chapter Five
Members and Observers of the Article 29 Data Protection Working Party

MEMBERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2007

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/
Bulgaria	**Cyprus**
Mr Krassimir Dimitrov Commission for Personal Data Protection – CPDP (Комисия за защита на личните данни) 1 Dondukov - BG - 1000 Sofia Tel: +359 2 940 2046; +359 2 915 3501 Fax: +359 2 940 3640 E-mail: kzld@government.bg Website: http://www.cdpd.bg	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
Czech Republic	**Denmark**
Mr Igor Nemec Office for Personal Data Protection (Úřad pro ochranu osobních údajů) 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/	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

Estonia	**Finland**
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	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 166700 Fax: +358 10 36 166735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi
France	**Germany**
Mr Alex Türk President of the 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 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	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

Greece	**Hungary**
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	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
Ireland	**Italy**
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	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 69 67 71 Fax: +39 06 69 67 77 85 E-mail: garante@garanteprivacy.it, f.pizzetti@garante-privacy.it Website: http://www.garanteprivacy.it
Latvia	**Lithuania**
Mrs Signe Plumina Data State Inspectorate (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	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

Luxembourg	**Malta**
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	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 2328 7198 E-mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt
The Netherlands	**Poland**
Mr Jacob Kohnstamm Dutch Data Protection Authority (College Bescherming Persoonsgegevens – CBP) Juliana van Stolberglaan 4-10, P.O Box 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	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: Sekretariat@giodo.gov.pl Website: http://www.giodo.gov.pl
Portugal	**Romania**
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	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

Slovakia	**Slovenia**
Mr Gyula Veszelei Office for the Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky) 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 62 19/20 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, goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
United Kingdom	**European Data Protection Supervisor**
Mr Richard Thomas Information Commissioner's Office Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel: +44 1625 545700 Fax: +44 1625 524510 E-mail: please use the online enquiry form on 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 ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2007

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	**Republic of Croatia**
Mr Philipp Mittelberger Data Protection Commissioner (Datenschutzbeauftragter 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. Franjo Lacko Director Mrs Sanja Vuk Head of department for Legal Affairs Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka – AZOP) Republike Austrije 25, 10000 Zagreb Tel. +385 1 4609 000 Fax +385 1 4609 099 E-mail: azop@azop.hr or info@azop.hr Website: http://www.azop.hr/default.asp
The former Yugoslav Republic of Macedonia	
Mrs. Marijana Marusic Directorate for Personal Data Protection (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tel: +389 2 3244 760 Fax: +389 2 3244 766 Website: www.dzlp.mk, info@dzlp.gov.mk	

Secretariat of the Article 29 Working Party

Mr Alain Brun
Head of unit
European Commission
Directorate-General Justice, Freedom and Security
Data Protection Unit
Office: LX46 01/182 - BE - 1049 Brussels
Tel: +32 2 296 53 81
Fax: +32 2 299 80 94
E-mail: Alain.Brun@ec.europa.eu
Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

NE-AC-09-001-EN-C
DOI 10.2758/5204

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 summarised 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 978-92-79-10363-6
9 789279 103636