Twelfth Annual Report

of the Article 29 Working Party on

Data Protection

EUROPEAN COMMISSION

1830-6446

Twelfth 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 2008

Adopted on 16 June 2009

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

"Freedom belongs to those who conquer it." André Malraux

This twelfth annual report on data protection reviews the significant progress made during a particularly eventful and challenging year. It is also the first report which I have the honour of presenting as Chairman of the Article 29 Working Party, taking over from my colleague and friend Peter Schaar.

This report is especially important as it reflects the remarkable work done by the various national delegations within the Article 29 Working Party in 2008. It recounts the particularly effective synergy which has allowed the adoption of stances crucial for the protection of individual liberties.

Faced with new complex issues related to the extraordinary development of information systems, our group has forged a doctrine of its very own, by synthesising concepts shared by the various national data protection authorities. It has overcome certain differences of interpretation to focus on building a common foundation of values and principles which it believes deserve special protection.

In particular, four strategic issues have been given our attention during 2008.

The protection of children's personal data is one of the central themes of our work programme. This concern mainly results from the development of social networks on the Internet and the new behaviours they bring about. The specific situation of children, their vulnerability and development, required the group to focus on these issues and identify appropriate solutions.

This has been done since the adoption of the WT147 notice of February 2008. Our group presented a structured summary of concerns relating to the protection of children's personal data, with a view to defining the basic principles that apply to children and clarifying their practical implementation in school settings. However, the subject has not been exhausted and other developments will inevitably follow. For now, the progress that our group has made so far constitutes an essential common basis for our future work.

Search engines are another key subject on which we are working. In our information society, Internet search engine providers have become an everyday part of the lives of Internet users and, therefore, play an important intermediary role in the provision of free access to information.

However, the huge amounts of user data they collect, process and store each day has a significant impact on the protection of users' personal data. Therefore, a joint reflection and precise framing of these practices was necessary.

In its joint recommendation WT 158 of April 2008, our group established rules to strike a balance between the legitimate interests involved. This recommendation was an opportunity to build a framework for action directed at search engine providers in which their obligations are clearly defined. It has also served to reiterate the rights of users in terms of the right of access or correction.

The recommendation which has been adopted is an important step forward in protecting the privacy of users. This is especially significant as search engine providers such as Google have already implemented the recommendations it contains.

Our group has also continued its work with regard to the international transfer of personal data from the European Union destined for subsidiaries located across the world. It has been responsible for optimising the understanding of existing tools by proposing a framework for binding corporate rules (BCRs) intended to facilitate their implementation by multinationals.

Finally, in terms of passenger information, with regard to the transfer of air passenger name record (PNR) files to the United States authorities, we have also worked hard to design information sheet templates tailored to the realities of the airline industry. The aim was to update the existing systems and facilitate the work of travel agencies, airlines or any organisations providing services to passengers flying to and from the United States.

These various projects and the solutions that have emerged all illustrate our resolute commitment to the protection of personal data. The current trend of intruding into the private lives of European citizens is a very real threat requiring clear, stable solutions and the definition of inviolable limits.

Alex Türk

Chapter One
Issues addressed by the Article 29 Data Protection Working Party[1]

[1] All documents adopted by the Article 29 Data Protection Working Party can be found under http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm

1.1. TRANSFER OF DATA TO THIRD COUNTRIES

1.1.1. Passenger Data / PNR

Opinion 2/2007 (WP 151) on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008

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. This opinion and the annexes update and replace the previous opinion of 30 September 2004 (WP 97). The current legal framework for transferring PNR information to the US authorities is covered by the agreement of July 2007. There remain obligations on travel agents, airlines and other organisations to provide information to passengers about the processing of their personal information, and 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. The short and very short information notices give passengers summary information about transfers of their data to the US authorities, and how to find out more information. The longer notice is in the form of frequently asked questions and provides more details about processing. It explains passenger data more broadly, before focusing on PNR data. It also includes links to the current agreement and other relevant documents.

1.1.2. World Anti-Doping Agency (WADA)

Opinion 3/2008 (WP 156) of the Article 29 Working Party on the World Anti-Doping Code draft International Standard for the Protection of Privacy

The European Commission's Directorate for Education and Culture (DG EAC) requested an opinion from the Article 29 Working Party on the draft international standard on the protection of privacy prepared by the World Anti-Doping Agency (WADA). The draft Standard should be read in conjunction with the World Anti-Doping Code of WADA, and Article 14 in particular. The Code requires that athletes regularly communicate specific data to anti-doping organisations. These data will be later stored together with other data (including sensitive data), in a database called ADAMS, located in Canada. Data relating to their support staff and other categories of people are also processed under the obligations envisaged by the Code. In its Opinion, the WP 29 pointed out the provisions of the Code raising questions of compatibility with European data protection standards. Concerning the WADA International Standards, the WP 29 addressed several issues dealing with the quality of processing of the relevant data, the consent of the data subjects, the information provided to them, the disclosure of personal data to third parties, the security obligations and the rights of the data subjects.

1.1.3. Binding Corporate Rules (BCRs)

Working Document (WP 153) setting up a table with the elements and principles to be found in Binding Corporate Rules

In order to facilitate the use of Binding Corporate Rules (BCRs) by a corporate group for its international transfers from the EU to organisations within the same corporate group, the Article 29 Working Party has created a table:

- clarifying the necessary content of BCRs as stated separately in documents WP 74[2] and WP 108[3];
- making the distinction between what must be included in BCRs and what must be presented to Data Protection Authorities in the BCRs application (document WP 133[4]);
- giving per principle the corresponding text references in documents WP 74[5] and WP 108[6] for further details; and
- providing explanations/comments on the principles one by one.

Working Document (WP 154) setting up a framework for the structure of Binding Corporate Rules

The Working Party has already established that international transfers of personal data from the EU but within the corporate group can take place on the basis of Binding Corporate Rules (BCRs) and has provided guidance on what the necessary elements of those rules are in documents WP 74[7] and WP 108[8].

To try and further assist and guide organisations in developing BCRs, the Working Party has developed a framework which is a suggestion of what the BCRs might look like when incorporating all of the necessary elements identified in documents WP 74[9] and WP 108[10].

Working Document (WP 155) on Frequently Asked Questions (FAQs) related to Binding Corporate Rules

As explained in Working Paper 74 (WP 74)[11], the Article 29 Working Party considers that BCRs are an appropriate solution for multinational companies and other such groups to meet their legal obligations and ensure a proper level of protection of personal information when transferring data out of the European Union. The Working Party/Data Protection Authorities have published a set of FAQs in light of their experience of the applications made for approval of BCRs and enquiries received about the interpretation of documents WP 74[12] and WP 108[13]. The FAQs are intended to clarify particular requirements for applicants in order to assist them in gaining approval for their BCRs. These FAQs are not exhaustive and will be updated as required.

1.2. ELECTRONIC COMMUNICATIONS, INTERNET AND NEW TECHNOLOGIES

Opinion 1/2008 (WP 148) on data protection issues related to search engines

Search engines have become a part of the daily life of individuals using the Internet and information retrieval technologies. In this Opinion, the Working Party recognises the usefulness of search engines and acknowledges their importance and identifies a clear set of responsibilities under the Data Protection Directive (95/46/EC) for search engine providers as controllers of user data. As providers of content data (i.e. the index of search results), European data protection law also applies to search engines in specific situations, for example if they offer a caching service or specialise in building profiles of individuals. The primary objective throughout the Opinion is to strike a balance between the legitimate business needs of the search engine providers and the protection of the personal data of Internet users. This Opinion addresses the definition of search engines, the kinds of data processed in the provision of search services, the legal framework, purposes/grounds for

[2] Working Document WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

[3] Working Document WP 108: Establishing a model checklist application for approval of Binding Corporate Rules, adopted on 14 April 2005 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

[4] Working Document WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm

[5] See footnote 2.

[6] See footnote 3.

[7] See footnote 2.

[8] See footnote 3.

[9] See footnote 2.

[10] See footnote 3.

[11] See footnote 2.

[12] See footnote 2.

[13] See footnote 3.

legitimate processing, the obligation to inform data subjects, and the rights of data subjects.

A key conclusion of this Opinion is that the Data Protection Directive generally applies to the processing of personal data by search engines, even when their headquarters are outside the EEA, and that the onus is on search engines in this position to clarify their role in the EEA and the scope of their responsibilities under the Directive. The Data Retention Directive (2006/24/EC) is clearly highlighted as not applicable to search engine providers. This Opinion concludes that personal data must only be processed for legitimate purposes. Search engine providers must delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times. The consent of the user must be sought for all planned cross-relation of user data and for user profile enrichment exercises. Website editor opt-outs must be respected by search engines and requests from users to update/refresh caches must be complied with immediately. The Working Party recalls the obligation of search engines to clearly inform the users upfront of all intended uses of their data and to respect their right to readily access, inspect or correct their personal data in accordance with Article 12 of the Data Protection Directive (95/46/EC).

Opinion 2/2008 (WP 150) on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)

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 the Proposal is 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. The Article 29 WP commented on the Proposal and addressed some additional issues, mainly concerning the notification of security breaches, the concept of "personal data", the concepts of "public communications network" and "electronic communications services", the National Regulatory Authorities (NRAs) and unsolicited communications.

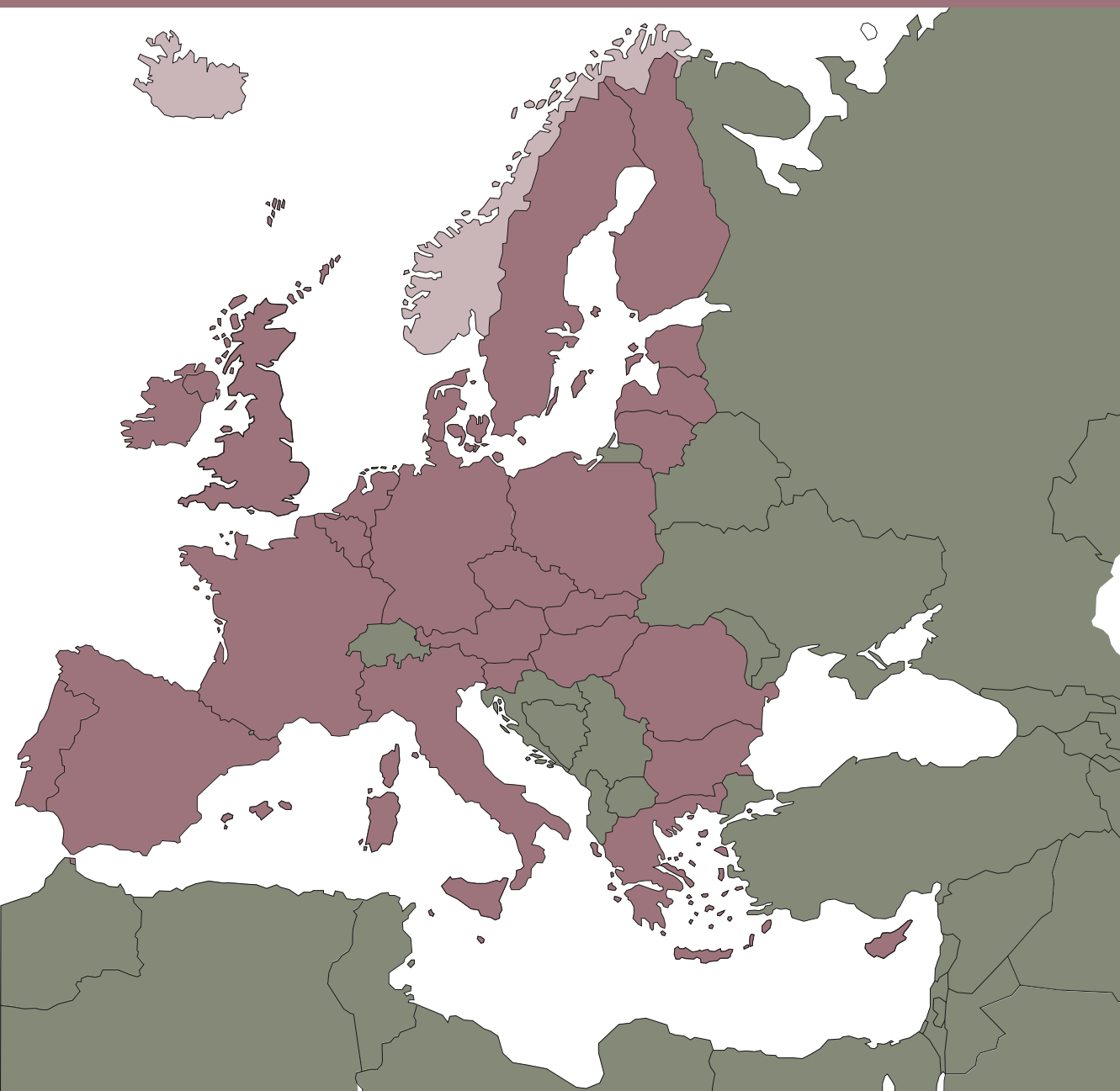
1.3. PERSONAL DATA

Working Document 1/2008 (WP 147) on the protection of Children's Personal Data (General guidelines and the special case of schools)

This opinion is concerned with the protection of information about children. It is aimed primarily at those who handle children's personal data. In the context of schools, this will include teachers and school authorities in particular. It is also aimed at national data protection supervisory authorities, who are responsible for monitoring the processing of such data.

The Article 29 Working Party, which has already adopted several opinions related to this issue. Its opinions on the FEDMA code of conduct (Opinion 3/2003); on geolocation (Opinion 5/2005) and on Visa and Biometrics (Opinion 3/2007) include certain principles or recommendations concerning children's data protection. The aim of this document is to consolidate this issue in a structured way, by defining the applicable fundamental principles and illustrating them by reference to school data. The area of school data was chosen because it is one of the more important sectors of children's life, and comprises a significant part of their daily activities. The importance of this area is due also to the sensitive nature of much of the data processed in educational institutions.

Chapter Two
Main Developments in Member States



Austria

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

A project of amendments to **the Austrian Data Protection Act** of 2000 (Datenschutzgesetz 2000) was planned in 2008. A draft was circulated early in 2008 and comments were collected[14]. However, general elections in the autumn of 2008 put an end to the project, which has not yet been re-entered into the legislative process. The draft addressed the following issues, among others:

- The current Datenschutzgesetz 2000 as regards a **legal person or group of natural persons as data subjects**. The draft would limit protection to natural persons. This suggestion received a mixed response; the Austrian Bar Association remarked that many companies needed the right to access and the right to rectification and erasure just as much as natural persons to protect their interests and had no alternatives granted by other laws.
- The draft contains provisions for a **data protection officer** for (larger) companies.
- The draft contains major changes regarding **notification**. It was planned that all notifications should be made online, using a new, exclusively electronic notification system. In the interest of speeding up notification procedures, material checking of notifications would be limited to prior checking cases.
- A completely new regulation should have addressed **video surveillance**. The data protection commission has received so many complaints and notifications that a more detailed regulation in law for video surveillance (especially video surveillance by private parties) appears necessary.

The **Data Retention Directive 2006/24/EC** had not been implemented in 2008. After the EC passed its ruling on the legal basis of the Data Retention Directive new endeavours have been started for implementation.

[14] The draft itself and all comments can be seen on the website of the Austria parliament: http://www.parlament.gv.at/PG/DE/XXIII/ME/ME_00182/pmh.shtml

B. Major case law

The first "**whistle-blower**" case was decided in late 2008. The Data Protection Commission considered - after long discussions - the Austrian affiliate to be the controller of data transferred to a US parent company via a whistle-blowing system. The reason why this legal view was adopted is as follows:

The employees of the Austrian affiliate were mandated by their employer in their labour contract to follow a specific Code of Conduct (this Code was binding for all employees of all companies within the group). The Code contained - among many other duties - the duty to report on certain unethical or even illegal situations coming to the knowledge of an employee. Making use of the whistle-blowing hotline was named as one of the possibilities of reporting said situations. An employee reporting via the whistle-blowing hotline thus follows general instructions given by his employer – he acts as an employee of the Austrian affiliate and not as a private person. Data transfers by employees are to be attributed to the employer as controller, especially if they are mandated by the employer (Case number K178.274/0010-DSK/2008).

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

C. Major specific issues

Video Surveillance
Video surveillance has been a major topic both in the form of complaints against video surveillance as well as in the form of notification cases:

A decision on the right of access to a video surveillance file, which had not been exploited, might be of general interest.

A citizen demanded the right of access to the video file of a public transport authority. The video data are deleted after 48 hours in this system unless a case of assault or vandalism occurred. The citizen was refused access by the controller (transport authority).

The data subject´s complaint to the Data Protection Commission was dismissed for the following reasons:

In order to grant access to the video surveillance data it would have been necessary to examine data recordings which otherwise would have been deleted un-examined after 48 hours. Moreover, the examination necessary for deciding whether the image of the complainant was among the surveillance data, would have revealed data about all other persons on the file whose data otherwise would have remained secret and would have been deleted after 48 hours.

Considering the fact that in Austria video surveillance files may only be exploited in a situation where surveillance was permitted (e.g. vandalism), it was ruled that access to non-exploited files would not be granted if the data in the file were deleted after a very short period of storage (e.g. 48 hours) and there was a high probability of other persons being visible in the file, so that granting access to one person would infringe the data protection rights of a multitude of other persons (Case number K121.385/0007-DSK).

Two notification cases involved video surveillance in schools. The Data Protection Commission did not permit video surveillance as a means of securing order inside the school buildings (this being an educational task to be performed by the teaching staff) but permitted video cameras in some areas outside the buildings as a means to protect property, e.g. to prevent bicycle theft (Case numbers K600.054-001/0002-DVR/2008 and K600.055-001/0002-DVR/2008).

Credit Reporting
Complaints against the credit reporting agencies remain high on the agenda of the Data Protection Commission.

Private Health Insurance
The Austrian data protection commission launched an audit of the private health insurance sector in 2008. The necessary recommendations will be passed shortly.

Belgium

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

No significant developments appear to warrant mention here.

B. Case law

The courts have not delivered any particularly important judgments warranting mention, with the exception of the position expressed by the Council of State according to which: pursuant to Article 7(3) of the *Privacy Act* (Act of 8 December 1992, relating to the protection of privacy with regard to the processing of personal data)[15], all draft royal decrees concerning the processing of data relating to health must be discussed at the Council of Ministers and referred for the opinion of the Commission for the Protection of Privacy (hereinafter the Commission or CPP) (Sectoral Committee on Social Security and Health - Recommendation 09/2008 of 27 February 2008).

C. Major specific issues[16]

Processing of sensitive data

Data relating to health - eHealth platform (Sectoral Committee on Social Security and Health - Recommendation 14/2008)

A new public agency endowed with the status of legal entity and known as the "eHealth platform" has been established within the Bank, at the crossroads of social security. The main aim of this platform is to provide an infrastructure and basic services for the secure exchange of health-related data between the different bodies in the health sector, and to function as an intermediary organisation responsible for collecting and coding data for historical, statistical and scientific research. The National Register number (unique identifier) and the social security identification number (derived from the National Register number) will be used for identification purposes on this platform. It will also hold a directory containing references, for patients who have given their consent, with information regarding which healthcare bodies hold what kind of personal data about them. This directory is used to channel data requests to the place where the requested data is available and ensure effective preventive control.

The Commission considered that this kind of decentralised platform, which merely conveys personal data but does not store any (with the exception of that contained in the directory of references) satisfactorily respects patients' privacy and complies with the recommendations of Group 29 *(Working paper 131 on the processing of personal data relating to health in electronic medical records).*

As for the use of the national registration number as the identifier for the platform, the Commission reiterated its general case law, which promotes the use of sector-based identifiers. It did not, however, object to its use in this case. Below we will address other issues related to the use of the national registration number, which, whilst not formally regarded as sensitive data, does nonetheless require its use to be safeguarded (Article 8(7) of Directive 95/46/EC).

Data on sentenced persons (Recommendation 28/2008)

Having received an increasing number of questions regarding sentenced persons within the framework of the exercising of parliamentary and press control, the Minister of Justice has sought the opinion of the Commission for the Protection of Privacy on the delicate subject of the relationship between data protection and the right to information. The right to information means that any member of parliament is entitled to ask the minister written and oral questions. Under parliamentary rules, questions concerning a personal case are, in theory, inadmissible. In the opinion of the Commission, the minister could therefore invoke these provisions in order to refuse to answer questions concerning data relating to a person who has a criminal conviction, but he could also choose to invoke the constitutional right to information to respond to the questioner. Under the *Privacy Act*, in theory, the processing of judicial data is prohibited, although an exception is made if the data is processed under the supervision of a public authority, if such

[15] The King determines, by decree deliberated in the Council of Ministers and taking into account the opinion of the Commission for the Protection of Privacy, special conditions applicable to the processing of personal data.

[16] All opinions, recommendations, permits and other documents cited in this paper are available on the website of the Commission for the Protection of Privacy at: http://www.privacycommission.be

processing is *necessary* for performance of its duties. In the opinion of the Commission, this exception applies to the processing of judicial data by the minister. Evaluation of the necessity of such processing will depend on the individual circumstances and the Commission states that it cannot issue a blanket recommendation on this point. In addition, the ban on processing judicial data does not apply to the processing of personal data intended for exclusively journalistic purposes when such processing involves data which has been made public by the person concerned or in close correlation with the public nature of the person or the events in which the person is involved. Here too the Commission concludes that everything depends on the individual circumstances and it can merely issue guidelines. It also refers to the constitutional provision which stipulates that judgments must be pronounced in open court. Therefore, if it was present during pronouncement of the judgment, the press will know about it. In this regard, the Commission considers that it is the responsibility of the judicial authorities to announce the content of a trial, through the 'press magistrate'. Finally, the Commission states that when a personal case refers to a matter that is mainly legislative, strategic or structural, the minister may disclose data with the aim of enabling a better understanding of the problem. He will, however, still be responsible for determining, on a case-by-case basis, whether or not an issue goes beyond the individual context. Where this is not the case, the Commission believes that a degree of reservation is called for.

The processing of sensitive data and the implementation of an anti-discrimination policy (Recommendation 05/2008)

In accordance with its policy of equal opportunities and diversity, the Flemish Office for Employment and Vocational Training wanted to investigate the presence of both foreign-born persons and persons suffering from a disability in its personnel records. Under what conditions would it be permissible, in accordance with Belgian privacy law, to implement a system to monitor these categories? The Commission concluded that data relating to diversity was sufficiently transparent and proportionate and was processed on a voluntary basis. The aims of the processing of this data were deemed to be legitimate, based, *inter alia,* on the rights and obligations established in legislation regarding proportional participation in the labour market. The Commission did, however, note a number of shortcomings which it requested be corrected before the monitoring system becomes operational:

- staff must be able to withdraw their consent or refusal, this change may not be permanently stored in the system;
- the period of implementation of the self-registration system has been badly chosen because it coincides with the period of staff assessment, which may give the impression to members of staff of the groups concerned that they are under pressure to divulge their data;
- given that the equal opportunities and diversity policy does not focus on any specific nationalities, the commission considers that immediately requesting the nationality of the parent(s) or grandparent(s) of staff members is excessive;
- staff must not be monitored on the basis of their nationality if the persons in question have not voluntarily registered as such for the monitoring purposes of this project.

Finally, the Commission stresses that the data processed is sensitive data. It recommends that the entire project be overseen by an information security consultant who will have particular responsibility for data protection tasks (assigned to data protection within the meaning of the directive).

Processing of sensitive data and anti-discrimination study

With regard to a recommendation (02/2008) addressed to a public company in the housing sector wishing to conduct a sociological study of (candidate) tenants, the Commission stated that the "birthplace" and "nationality" data did not appear to necessarily be sensitive data. Their collection should nevertheless remain pertinent. With regard to this point, the author of the study cited an aim *of social diversity and the fight against discrimination in the housing sector.* In response to this argument, the Commission pointed out that, in accordance with anti-discrimination legislation, a distinction made on any grounds accepted as discriminatory does not necessarily constitute discrimination as long as it is objectively justified by a legitimate aim and means of achieving that aim are appropriate and necessary. Moreover, a precise definition of the purposes and criteria for their

attribution is of the utmost importance when potentially sensitive or discriminatory data is being processed. The Commission advised that the legislation applicable to the party making the request calls for a clearer definition of the purposes (fight against discrimination) and of the data to be processed. Citing commitment to anti-discrimination in a general way is insufficient.

In the same recommendation, the Commission states that consideration of the viability of subsequent processing by a data controller within the public sector must be based on laws and regulations which adequately describe the subsequent processing, as well as the types of data that can be processed, their origin and the reason for their use. The adoption of an *ad hoc* decree or regulation might suggest that such subsequent processing is not incompatible with the initial processing. Failing that, the relevant conditions established by the implementing Royal Decree (13 February 2001) of the *Privacy Act* will apply.

In 2008, the Commission has also taken several initiatives in relation to data processing within the context of research. Some of these are described below.

Historical, statistical and scientific research

Researcher's handbook

In 2008, the Commission has, for example, published a researcher's handbook. In this publication, it informs the research sector of the rules and procedures to follow when collecting and analysing personal data for their research. The Commission distinguishes 4 steps for which it has identified a number of issues and made recommendations: before beginning research (principles governing the use of secondary data, the collection of sensitive data); whilst collecting data (information on first contact, refusal to participate and the removal of identification data of individuals who opt for this refusal, the collection process itself and the rights of access, rectification and deletion); during research and publication (the most thorough and rapid anonymisation possible, staff awareness, publications); and after research. Finally, the handbook also includes a Code of Conduct (see below) which recipients of data from the National Register agree to follow when carrying out their scientific research.

Code of Conduct for researchers using the National Register (Recommendation 27/2008)

The strict procedures for the protection of privacy established by the Commission in recent years were worrying researchers. The cumbersome conditions of access to the National Registry were giving rise to fears that they would no longer be able to undertake responsible scientific research. The Commission took these concerns seriously and conducted a study of this issue both internally and with the scientific research sector.

Within the framework of conducting scientific research based on a sample of the population and pursuing an outcome of general interest, any Belgian institution is entitled to the disclosure of identification data from the National Register, subject to permission from the competent sectoral committee. Written surveys are the rule, while oral surveys (in the presence of the person) are the exception. If the researcher cannot or does not wish to work by means of a written questionnaire, he must apply to the Sectoral Committee of the National Register and justify his choice. If the study involves written questionnaires for a single survey, the National Registry itself will send out the questionnaires, accompanied by an introductory letter and any documents provided by the research institute. Subsequent questionnaires may be sent out in line with the same procedure. In this case, the National Register will only pass on to the research body the data necessary to enable it to analyse the refusals to participate, and this information will only be provided in a coded form. In the case of oral surveys in which personal identification data is required, the National Register will pass on the relevant data to the research organisation, on the condition that it undertakes to respect the following rules:

- the person concerned may not be contacted more times than he/she wishes;
- the research institute must behave in a polite and professional manner;
- personal data must be subject to special protection, possibly with the assistance of a trusted third party;
- reports and publications made on the basis of research data obtained using information from the National Register may only contain anonymous data.

The reuse of administrative data for research purposes - trusted third parties (Recommendation 20/2008)
When asked for advice on reusing data from administrative databases of universities in order to follow the intersectoral and international mobility of researchers as well as the influence of a PhD on the labour market, the Commission requested the establishment of a *trusted third party* responsible for data matching. This requirement aims to ensure a barrier between, on the one hand, the entity within which administrative data is collected and matched and, on the other hand, the research institute which will only receive anonymised data for the purpose of scientific and statistical study. In the meantime, the internal unit responsible for the matching must meet the following requirements:

- external monitoring of the internal matching process must be organised;
- management of the internal unit must be performed by a body that represents the different categories of persons whose data is being processed;
- in accordance with the Privacy Act and its implementing Royal Decree, the matching unit must be regarded as an autonomous data controller (and not as a subcontractor for various data providers) and assume the corresponding responsibility;
- the matching unit must anonymise the data so that the research unit cannot itself establish a link between the information obtained and an identified or identifiable individual.

In the recommendation relating to the eHealth platform, which has already been mentioned, the Commission had, similarly, stated that the role of eHealth as an intermediary organisation was to ensure encoding by an independent, neutral third party, for the purpose of historical, statistical or scientific research. The Commission stresses the importance of the fact that the intermediary organisation must not itself undertake any research.

Private sector - commercial and financial activities
SWIFT
In a decision dated 8 December 2008, the Commission put an end to the recommendation procedure initiated against the company SWIFT (see also the 2007 and 2006 annual reports). Several factors which characterised the course of the proceedings and several factors regarding the decision reached by the Commission should be highlighted:
SWIFT collaborated honestly and unreservedly in the fact-finding process, allowing the Commission to access all useful information and documents. The Commission was therefore able to determine with precision the respective persons responsible for various clearly identified operations (the uncertainty that had prevailed until now was mainly due to the complexity of and unfamiliarity with the system). Now, the banks, the financial community and SWIFT each have specific obligations to perform - as data controllers - in order to ensure the protection of the personal data inherent in the execution of financial transactions.

SWIFT has agreed to recognise and assume certain clearly defined responsibilities. It has declared those responsibilities, on its own initiative, to the public register kept by the Commission, thereby complying with the legal obligations that demand transparency in the processing of personal data.

The Commission also noted that in response to the accusations made against it, SWIFT has adopted a series of measures intended to better prevent certain risks and enhance protection of the personal data it processes: a new architecture for its international network and the setting up of a processing centre in Switzerland to manage messages within Europe (which will no longer be transferred to the USA); the appointment of a full-time "Privacy Officer" within the company, who has been given specific powers and tasks; formalisation of procedures for the supervision, referral and monitoring of requests from people whose data is being processed; formation of a permanent data protection working group responsible for assessing and adapting existing protection measures; the development of an accessible information policy, etc.

Direct marketing
In June 2008, the Commission took the initiative to publish a legal notice on the issue of direct marketing. To better protect privacy in the context of data processing

for direct marketing purposes, the Commission highlights the following points:

- it is essential to make a clearer distinction between direct marketing on a (pre-)contractual basis - direct marketing used as part of normal management of customers - and other forms of direct marketing regarding which the Commission receives numerous complaints;
- the legitimate interest of the entity responsible for the data processing (Article 5(f) of the LVP - Article 7(f) of Directive 95/46/EC – the invocation conditions of which are specified) - should not be regarded as a residual basis after Articles 5(a) and 5(b) of the LVP (Articles 7(a) and (b) of Directive 95/46/EC);
- consent is stipulated as a condition for the brokering of addresses and profiling for direct marketing purposes, for data processing which is not *a priori* legitimate by direct contact with the person concerned;
- the notion of (non-)compliance with the principle of honesty has been explained with the help of concrete examples;
- the term "incompatible use" has been defined as has the need for a retention time limit;
- based on the principle of honesty, the Commission calls for a duty of proactive notification at the source of a direct marketing campaign where there is no direct contact with the person concerned (e.g. in the case of data trading). The Commission urges caution when using standard notification rules and insists that the corresponding information must be as clear and comprehensible as possible.

This notice is currently the subject of a consultation with the sector and may, depending on the comments received, be amended in the future.

Negative lists

As in previous years, the issue of blacklists has been at the heart of the concerns of the Belgian Commission. Recommendation 34/2008 regarding a draft law on the supervision of negative lists summarises the constant point of view of the Commission throughout nine recommendations since 1998:

- negative lists constitute a form of interference in private life which is contrary to Article 8 of the European Convention on Human Rights;
- only the legislative authority has the power to "authorise" such lists; the Commission therefore invites the legislature to supervise the unregulated negative lists in existence;
- the essential elements of any negative lists must be established by law. This particularly applies to defining their aim, conditions of recording, situations and conditions under which the data controller can validly justify the processing by virtue of Article 5(f) of the LVP (Article 7(f) of Directive 95/46/EC), the nature of the data, the retention time limit, data dissemination and access to data;
- the purpose of negative lists should be clearly set out; the aims of "fighting fraud" or "protecting security" are not sufficiently precise;
- a duty to declare negative lists to fight discrimination;
- a single authorisation system and a declaration of conformity based legal principles, as is already largely the case in France;
- the introduction of a reciprocity guarantee in the exchange of personal data with other countries of the European Union that apply stricter rules, particularly for multi-sectoral negative lists and sectoral "zero-tolerance" lists.

Privacy and the right of ownership

In 2008, the Commission has regularly been consulted on the application of the Privacy Act in the area of forced co-ownership of condominium buildings. These issues came both from the managing agents of buildings (whether professional or not) as well as sometimes directly from the co-owners themselves. In its recommendation 22/2008, the Commission found that the co-ownership association should be considered responsible for the different processing carried out by the management body, its agent, within the context of or in connection with the co-ownership management. The recommendation also concludes the legality of certain specific types of processing regarding the disclosure, by the management body to the co-owners, of names and addresses of other co-owners as well as disclosure to all co-owners of the account status (allocation of expenses and charges) of each individual owner. Finally, the Commission for the Protection of Privacy encouraged the adoption of sectoral or professional codes of conduct.

Identification issues

Belgium has long opted for a single identification method, the national registration number, access to and use of which is strictly regulated. A committee (the sectoral committee of the National Register) partly composed of members of the Commission is responsible for authorising this access and its use in accordance with strict safeguards.

Managing users and access (Recommendation 01/2008)

in 2008, the Committee of the National Register received several requests for permission to use the national registration number for the purpose of managing user access. As this is a widespread issue, the case has been referred to the Commission. The Commission has issued a general recommendation, which contains several practical rules for the management of such access within the public sector:

- it is recommended that a system be developed based on the principle of circles of trust;
- there should be a high quality registration process, which involves verifying the identity of the user who is connecting, his characteristics and authorised representatives, supported by validated authentic sources (which provide guarantees as to the accuracy of the data);
- there must be electronic identity authentication, preferably using the electronic identity card;
- the management of access includes recording and checking permissions.

How to access the National Register

A 2008 law entrusts banks and insurance companies with the duty of searching for the holders of dormant accounts and safe-deposit boxes, as well as the holders of dormant insurance policies. In order to find and contact those people, the consultation of records such as the National Register is authorised. In Recommendation 31/2008, the Commission expressed its satisfaction with the planned set-up for access to records, as they are not made directly available to banks. A *central point is responsible for gathering reasoned requests for access* from banks and insurance companies and then sending a response to them. This type of set-up (access to the National Register for a given sector via a central point which provides controlled access for the sector) makes it possible to prevent any improper access to the data in the records concerned and any misuse by banking and insurance institutions.

Use of the electronic identity card (Sectoral Committee of the National Register Recommendation 02/2008)

The Committee of the National Register has been asked to respond to a series of questions relating to the use of the electronic identity card (eID). Although the Commission considers the eID to be the ideal tool for identification, it reiterates the legal conditions under which its presentation may be requested. These presentation conditions exclude the compulsory use of the eID as a library card. While citizens remain free to choose to use their eID card as library card, this cannot be imposed. No benefits available to holders of different types of library cards may be linked to the use of the eID as a library card.

Public Sector

Central Register of Vehicles

Since 2006, the Commission has issued several (negative) recommendations relating to the creation of an authentic source of data regarding vehicles. In its Recommendation 23/2008, it reiterates that its data controller must be clearly identified and that centralised storage and logging subject to external federal control seems to be the option that offers the most safeguards in terms of personal data protection. The Commission also noted that the Sectoral Committee for the Federal Authority[17] must grant permission for flows of electronic data from the federal institution (DIV - Vehicles Department) that will host this database. In this regard, the Commission did not express its support for the creation of a new "Mobility and Transport" sectoral committee, but rather advised that the greatest possible consistency with existing sectoral committees be aimed for.

Meanwhile, in the absence of an adequate legal basis, the disclosure of personal data from the Central Register of Vehicles must be authorised and in order to comply with the *Privacy Act*, the conditions of such disclosure must be stipulated in public procurement contracts and concession agreements entered into with concession holders.

[17] This Sectoral Committee is competent to authorise any electronic disclosure of data from a federal authority.

Federal service integrator (Recommendation 41/2008)
In the course of 2008, the Commission also issued a recommendation on a draft law regarding the establishment and organisation of a *federal service integrator*. The evaluation of this initiative, for which the Commission had already spoken in favour in the past, was positive, especially the option taken for a *service integrator*, deemed less threatening in terms of data protection than data integration. The Commission has nevertheless stressed the importance of the concepts of authentic sources and data, the principle of single collection, and the necessary transparency to the citizen (the possibility of being able to check who has accessed data concerning him).

Flemish decree on the electronic exchange of administrative data (Recommendation 01/2008)
As this decree was primarily designed to fill a gap that had important repercussions on the protection of privacy, specifically the absence of thorough checking of the electronic exchange of data between services attached to federal institutions, the initiative has been welcomed by the Commission. The Commission did, however, regret that this checking has not been entrusted to a sectoral committee established or to be established within the Commission but rather to an autonomous Flemish commission, outside of the Commission, whose independence does not appear to be guaranteed. In this regard, it stressed that this option would complicate the exchange of data between authorities at different levels of power and give rise to a risk of divergent jurisprudence. The decree finally adopted clearly took into account the remarks made by the Commission. In order to ensure its independence, the Flemish commission was established by the Flemish Parliament and a close link has been organised with the Commission as three of its members are now also part of this new federal commission.

New technologies
Data retention (Recommendation 24/2008)
In 2008, the Commission issued a recommendation aimed at incorporating into Belgian law the European Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks. The objective of this Directive is to harmonise the obligations placed on providers in terms of the retention of certain data and ensure that said data is made available for the investigation, detection and prosecution of serious crimes as defined by each Member State in its domestic law. For various reasons, the Commission issued a negative opinion, mainly due to the failure to mention the essential elements for the retention of data (type of data stored, the retention period, storage methods, reasons for storage, type of criminal acts whose punishment justifies the use of retained data, purposes, etc.).

Public Information
Also in 2008, the Commission developed several pages of its website in English, notably informing citizens of its international activities in this area in English as well as French and Dutch.

Bulgaria

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

From the beginning of 2006, Directive 95/46/EC of the European Parliament and of the Council 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, has been fully implemented through the Law for Protection of Personal Data (LPPD). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, was implemented in Bulgarian legislation through the Law on Electronic Communications (LEC) promulgated in State Gazette No 41 in 2007.

In 2008, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC was implemented in Bulgarian legislation through Ordinance No 40 of 7 January 2008 issued by the Minister of the Interior and the Chair of the State Agency for Information Technology and Communications promulgated in State Gazette No 9 of 29 January 2008, on the categories of data and the procedure for their retention and provisions by the undertakings providing public electronic communications networks and/or services, for the purpose of national security and crime detection.

B. Major case law

In 2008, the specific cases of violation of Directive 95/46/EC and the Law on Personal Data Protection were related to personal data processing, which exceeded the legally defined purposes, including cases of further processing in an incompatible way. In such cases, it is established that the personal data controllers require a copy of the individual's identity when providing certain types of services. This was the case for some complaints against actions involving the provision of public electronic communications networks and/or services under the Law on Electronic Communications, which the Commission for Personal Data Protection has been considereding.

Specific cases of unauthorised personal data processing involved the use of personal data of insured individuals when changing pension insurance companies. In these cases the individuals clearly state that they have not submitted applications for change and have never signed any application form nor certified their signatures before a notary. According to the procedure for transfer of insured persons from one pension insurance company to another, every pension insurance company enters into contracts with physical or legal persons registered in the Financial Supervision Commission as insurance agents. In case of a request for change, the insured person has to sign the application and his/her signature is certified before the notary. The application is submitted to the company to which the individual wishes to be transferred, where only a check on the requisites is performed. The practice of the Commission for Personal Data Protection is aimed at enhancing the control exercised by the pension insurance companies on the insurance agents in their capacity as personal data processors.

In 2008, the Commission for Personal Data Protection took actions on its own initiative with regard to the organisation of promotional events (quizzes, games and research of the purchasing interest in particular products) and the processing of participants' personal data in such initiatives. It was determined that receiving a price was connected to the provision of additional personal data as well as that in order to participate in the initiatives a submission of personal data is required. In such cases, the Commission for Personal Data Protection has issued compulsory instructions for the personal data controllers in future invents to observe the principle of proportionality of the processed personal data and to depersonalise the collected data in future events.

The Commission for Personal Data Protection has issued opinions on the provision of access to the National Database "Population" of parties, to all those with a proper legal interest, including both persons and state authorities for the purpose of performed

actions laid down by law Opinions have also been issued regarding the definitions of "personal data controller" and personal data "processor".

The Commission has replied to many inquiries made by individuals about their rights under LPPD and the obligations of the personal data controllers. These inquiries have had the form of e-mail, letters and in person. Many of the received questions in the CPDP relate to the way in which the individual's rights are protected by the processing of his/her personal data and the provision of access to them.

The opinions and the specific questions and answers of the Commission on the application of the Law are published in the CPDP bulletin on the official website: www.cpdp.bg.

In 2008, in connection with a twinning project financed by Phare programme and jointly with experts from the Spanish Agency for Data Protection, a planned inspection was carried out in the bank sector. From this inspection it was established that bank clients are informed about the data (which identify the controller and its representatives), are acquainted with the personal data processing purposes, and receive information that their data will be transferred to third parties. However, clients are not always notified about the receiving parties or categories of receiving parties to which their data may be disclosed. There have also been cases in which the clients are not informed whether the provision of information is obligatory or voluntary and the consequences that would result in case of data controller's denial.

C. Major specific issues

In connection with the registration of the records kept by personal data controllers, performed by the Commission for Personal Data Protection, along with the traditional submission of registration documents on paper, at the start of 2008 a system known as eRALD was introduced for the first time for electronic registration of personal data controllers. eRALD is a web-based application which enables all controllers to enter their own data and start the registration process or make changes to the entered information. The controllers receive their username and system password and the procedure initiated by them is under their complete management and control. They carry full responsibility for the accuracy of their data and for keeping this data up to date. The entered data are locked for access until registration is complete.

The implementation of an electronic registration system is one of the greatest successes of CPDP, because it enables the process to be substantially eased and simplified and the registration time to be much reduced. In addition, it provides greater stability and legal certainty.

During the whole year, the Commission for Personal Data Protection participated actively in the work of the specific "Personal Data Protection" group, created as part of the Council of Ministers joint working group, with the purpose of undertaking the necessary actions to ensure full implementation of the provisions of the Schengen *acquis*. In the framework of this initiative, the Commission for Personal Data Protection discussed in work meetings the experiences of the new Schengen countries, exchanged experiences, familiarised itself with training programmes, carried out inspections of the central SIS database, performed research into the application of the legal basis, discussed cooperation between the national data protection authorities and the influence of the enlargement of the Schengen area.

On 5 December 2008 in Brussels, at the meeting of the Council of the European Union "Schengen Evaluation" Working Expert Group, Bulgarian experts from the Ministry of the Interior, Ministry of Foreign Affairs and the Commission for Personal Data Protection presented the summarised answers of the "Schengen Evaluation" questionnaire. This opened the first stage of the accession procedure of the Republic of Bulgaria in the Schengen area - a main priority and challenge for our country after its accession to the European Union.

At the end of 2008, the European Commission approved a Project Fiche (BG-2007/019-303.07.03.01), which includes the execution of one component- the Twinning Light Project (BG/2007/IB/JH/01/UE/TWL): "Cooperation for Additional Administrative Strengthening of the

Bulgarian Commission for Personal Data Protection and for Further Improvement of the Control Activity in the Field of Sectorial Audits".

The partner selection procedure has now been completed with the choice of the Spanish Agency for Data Protection. The execution of the set activities in the project is expected to start after the signing of the contract.

Cyprus

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

1. There were no legislative developments relating to the implementation of Directives 95/46/EC and 2002/58/EC.

There were discussions in the Parliamentary Committee of European Affairs, the Parliamentary Committee on Legislative Matters and the Parliamentary Committee of Human Rights regarding the implementation of the national data protection legislation, Law 138(I)/2001.

The discussion was followed by a Memorandum submitted by the Commissioner which dealt with:
- the evaluation of compliance with the legislation;
- public awareness;
- effectiveness of the exercise of the powers of the Commissioner and measures needed for this exercise to became more effective;
- problems and difficulties in the operation of the Office of the Commissioner (mainly relating to the recruitment of its staff).

For its part, the Parliamentary Committee on European Affairs issued a Report in which it commented, among other things, on the above issues, and made special mention of the role and contribution of the Working Party especially as regards the increasing use of personal data in the name of the fight against terrorism.

2. The Law transposing Directive 2006/24/EC on the retention of telecommunications data was amended so as to allow access to the retained data without a Court Order in cases of kidnapping.

A Court Order must however be obtained within 48 hours from the time of access to such data and, in case such an Order is not obtained, the police officer in charge must destroy the data obtained and notify the Commissioner for the Protection of Personal Data about this.

3. A Law on the prevention of violence in sport has been enacted which provides, among other things, for the establishment and operation of a database containing records of personal data regarding persons whose entry to the relevant sports ground has been prohibited, in order to fight and control violence in sports grounds, especially in football matches.

B. Major case law

A complaint was examined by my Office regarding the loss of a patient's file at Nicosia General Hospital. The hospital administration admitted that it could not find the file of the complainant. As a result a fine of €2000 was imposed.

After a complaint was submitted to my Office by a person claiming that his personal data which was in a database of the Ministry of Education and Culture had been unlawfully used by a student union for "marketing" purposes, we discovered that in the process of examination of the complaint, that the controller of the relevant database had retired two years before and that nobody had been appointed by the appropriate authority to replace him.

As this omission led to the fact that there was no person responsible for the lawful processing of the relevant personal data, we concluded that the Director-General of the Ministry was responsible for this omission and we imposed a fine of €1500.

C. Major specific issues

- During 2008, we continued to follow and review the steps taken by the New Nicosia General Hospital following our recommendations after the audit we conducted in 2007. We monitor the procedures established with respect to the security of and access to the personal data processed by the Hospital and we are kept informed of the progress in the establishment and operation of its IT system.
- There were several complaints about the use of CCTV in the workplace and the use of workers' fingerprints for checking their attendance at work. As we had already issued Guidance about these two matters,

we are checking on compliance of the controllers' actions with our specific directions.

- We also dealt with the question of teachers' access to their personal files and the categorisation of public servants' leave of absence so that applications for sick leave are for restricted use and kept in a separate file to which only personnel specially authorised in writing by the appropriate authority can have access.

The Czech Republic

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

The basic legal regulation in the area of personal data protection is provided by Act No 101/2000 Coll. on the protection of personal data and amendments to some related acts, which came into effect on 1 June 2000. The Office for Personal Data Protection ("OPDP" or "the Office") was established as an independent body on the basis of the provisions of this Act and is endowed with strong powers, being able to implement measures and directly impose fines in case of breach of law. The Act essentially implemented the Directive 95/46/EC into the Czech legal order. With effect from July 26, 2004, Act No 101/2000 Coll. was amended by Act No 439/2004 Coll., and was thus brought into full accordance with the aforementioned Directive.

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

In 2008, an amendment procedure of the Electronic Communications Act No 127 caused by the need to transpose the Data Retention Directive No 2006/24/EC into national law was completed.

When enforcing national law and by extension EU/EC law, control work, including on-the-spot inspections, continues to play a key role. The instigations that inspectors respond to can be divided into two basic groups: complaints regarding one-off violations of the law and complaints intimating that the law is being broken systematically. In the case of isolated violations the matter in question is often resolved during the "preliminary investigation" phase. In these cases a remedy may be imposed without a formal control. This approach cannot be used in all cases – it is usually applied in cases where the irregularity was not the result of a deliberate action. However, inspectors still deal with the vast majority of complaints by performing proper checks, including on-the-spot inspections.

Even though checks continue to be the main supervisory tool, increasing emphasis is being placed on raising awareness of personal data protection. Last year, for example, OPDP specialists gave 260 hours of lectures.

A programme prepared for teachers by the OPDP, which has received three-year accreditation from the Ministry of Education, Youth and Sports, has also been initiated. Seminars were conducted in the regions. In addition, the second annual art and literature competition for children and young people "My privacy! Don't look, don't poke about!" was held. This time, children from SOS villages in the Czech Republic, Ukraine, Kazakhstan, Russia and Bosnia-Herzegovina also successfully took part in the competition. The Office sincerely welcomes this cooperation, because it considers it necessary that children preparing for their future life while growing up outside a family are also sufficiently informed about their rights.

Following the international acclaim that the children's competition and teacher training project brought the Office in the previous year (Madrid, 2007, Prize for Data Protection Best Practices in European Public Services), the children's works were put on display in the entrance hall of the Palace of Europe in Strasbourg on the occasion of Data Protection Day.

The Office also continued to work with the third medical faculty of Charles University by holding a seminar dealing with the specific threat to privacy and data protection with respect to the elderly.

B. Major case law

As part of the *electronic filing of public administration* and the introduction of e-Government services, work continued on the preparation of legislation on the new electronic registers of public administration. The OPDP asserted fundamental comments and reservations and insisted that technical aspects be discussed and risks associated with the protection and securing of personal

data be assessed; consequently, the Office is often regarded as slowing down the process. Nevertheless, even though the Office did not manage to bring all its opinions to bear, its positive influence on the resulting solution is evident.

It also succeeded in having a positive influence on the preparation of the *Act on the 2011 census*. Here the Office's comments concentrated on ensuring that, in the new planned electronic census, in the work of the census officer and equally in the event of any cooperation with external entities, clear rules were put in place governing access to certain types of information and securing data against abuse.

By contrast, attempts to influence the working of *medical registers* were not so successful – the Ministry of Health did not accept the OPDP's request to fully clarify the concept of the central registers. The Office requested an explanation for the justification of the defined data storage period in the individual registers and for the reason why the consent of the affected persons is not taken into account, as is the case in certain other European states.

Not all the Office's suggestions were accepted when the *Act on conflict of interests* proposed by a parliamentary initiative was being drafted. Here the Office gained specific supervisory powers, but it continues to regard the fact that the Act does not distinguish sufficiently clearly between constitutional and other elected officials who, as public persons, have a fundamentally reduced guarantee of privacy, and public administration officials whose privacy protection must essentially be preserved with regard to matters not directly related to the conduct of their actual official duties.

C. Major specific issues

Control activities of OPDP in 2008 included a total of 112 completed controls related to DP Act No 101/2000 Coll. (the same as in 2007), plus 91 completed controls related to unsolicited commercial communications under the Act No 480/2004 Coll. on certain information society services. Most of the controls (inspections) performed by independent inspectors and their control teams were *ad hoc* actions based on instigations and complaints of individuals. Only a little more than 10 % of inspections is based on the Control Activity Plan, but these types of control action usually have a much more complex nature covering a wider scope of data processing features and aspects.

The *Control Activity Plan 2008* focused on 5 main general topics:

1. Personal data processing in the work of the justice and public prosecution authorities, with particular emphasis on the performance of execution and the courts' practice when maintaining the insolvency register;
2. Personal data processing with regard to the EU's joint information systems, namely the Customs Information System (CIS), Eurodac and the Schengen Information System;
3. Public administration information systems not classified elsewhere, focusing on diagnostic institutions, children's homes with schools and educational care centres, i.e. how institutions for children brought up outside standard family conditions process personal data, and also on the Ministry of Finance and the tax offices;
4. Personal data processing under surveillance systems in both the public and private sectors, namely in the buildings of the Ministry of Culture, hospitals, social care facilities and in the offices of private companies;
5. Personal data processing with regard to consumer protection, focusing on modern technologies enabling rapid identification, especially RFID systems.

Control work based on complaints and other instigations touched on a wide range of areas in both the public and private sectors. One major area was again public administration, where there are often problems with the use of the population records information system, for example. This source is used by many public administration authorities, both under the Act on population records and on the basis of several dozen special Acts; the Office often encounters attempts to make broader use of the data than these Acts permit.

Complaints also led to controls being performed in the healthcare system, where a number of breaches of the act on personal data protection were identified.

The Office paid particular attention to the processing of DNA-related personal data. A control was carried out in 2008 targeting the Institute of Criminalistics of the Police of the Czech Republic, the operator of the National DNA Database, which was set up in response to complaints and on the basis of the Control Plan from the previous period. Violations of the Act on personal data protection were found, as sensitive data were collected, processed and stored to an extent that went beyond the statutory authorisation. In such cases the law requires that the consent of the concerned person is obtained, but this had not occurred. One aspect of the control conclusions was the imposition of a fine and a remedy measure, namely the destruction of personal data processed in a manner contrary to the law.

Based on complaints and other instigations, a control targeted private companies performing genetic paternity and kinship testing for identification for commercial purposes, as well as DNA analysis for research and for the testing of genetically conditioned types of illness and predicting the efficacy of their treatment. Violations of several provisions of the Act (the duty of notification, consent that did not cover all use of data, certain aspects of proportionality, etc.) were found and a fine and remedy measures were imposed.

Surveillance (camera) systems in the public and private sectors continue to be the subject of numerous complaints and the subsequent controls. This is a growing trend, although there has been some small success (e.g. more restraint in the introduction of cameras in schools) brought about both by numerous controls and by intensive awareness raising by the Office in the form of opinions, consultations, etc.

The above-mentioned control activities do not include those concerned with **unsolicited commercial communications** ("marketing spam"). In 2008, this special agenda involved 1458 complaints and other instigations received by OPDP, of which 1311 were dealt with, 91 controls were completed and 81 sanctions imposed.

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 came into force on 1 July 2000. The English version of the Act 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 on 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 714 of 26 June 2008 on the Provision of Electronic Communications Network and Services;
- Chap. 71 of Law on Administration of Justice, cf. Exec. Order No 1069 of 6 November 2008;
- Section 263 of the Penal Code, cf. Exec. Order No 1068 of 6 November 2008.

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. In 2008 the DPA gave its opinion on several laws and regulations affecting privacy and data protection.

B. Major case law

In February 2008 a night club asked the DPA for an authorisation under Section 50 (1) of the Act on the Processing of Personal Data, to process data about their guests with the purpose of guaranteeing a safe and peaceful night-time environment.

In order to guarantee a safe and peaceful night-time environment the night club wished to implement the following initiatives:

- Create an electronic access control system using the guests' fingerprints (templates) and pictures.
- Create an internal list of guests who have been banned from the night club due to acts of violence, vandalism, threats and use and/or sale of drugs. The internal list would contain information about the length and grounds of the ban.

After presenting the case to the Council, the DPA concluded that the night club could process their guests' fingerprints (templates) and pictures with the explicit consent of the guest.

If the guest withdraws his or her consent the night club is obliged to delete the fingerprint and the picture.

The DPA also concluded that the night club could be given authorisation to process sensitive data (such as data concerning health (drug use) and criminal offences) according to the following terms:

- Processing of sensitive data in connection with imposing and administering a ban may only take place with the written consent of the guest. The consent must be explicit and has to be in accordance with the Act on the Processing of Personal Data. That means it has to be freely given, specific and informed.
- If the guest withdraws his or her consent, data concerning the reason for the ban must be deleted.
- The processing of sensitive data must be in accordance with the security measures specified and listed in an appendix.

Employees at the night club must be informed that their use of the banned guest list will be logged and

that the log can be used to locate unauthorised use of the banned guest list.

C. Major specific issues

In November 2007 it came to the attention of the DPA that underlying sensitive data pertaining to natural persons had been published in connection to publications of PowerPoint presentations.

This led the DPA to initiate several cases on its own initiative against public authorities and private controllers. Most of the cases started in 2007 have ended in 2008 with the DPA expressing criticism towards the controllers responsible for the publications.

Due to the security problem, the Danish DPA also requested that public authorities in Denmark make sure that their websites did not contain such embedded data pertaining to natural persons.

Furthermore, the DPA recommended that the public authorities should check whether such data had been disclosed to third parties in other ways, e.g. to participants in meetings etc. In case such disclosure had taken place the public authorities should take initiatives in order to withdraw the data or having the recipients delete it.

Description of the security problem and how to avoid it
The security problem arises when PowerPoint-presentations contain Excel graphs or tables in the form of an embedded object. By opening this object it is possible to gain access to the underlying data, which might contain sensitive data (to open the object you have to save the .ppt file on your PC, then open the object in your PowerPoint application and click on the graph or table in question).

The problem has mainly appeared in PowerPoint presentations, but can also be found in other kinds of Office files such as Word documents, if a file from another program (for example Excel) has been embedded.

The security problem can be avoided in the following manner:
1. The PowerPoint-presentation is converted into a .pdf format
2. Graphs and Tables are inserted as pictures and not as objects.

The same procedure is used when inserting graphs and tables into Word documents.

Estonia

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

During the accounting period of 2008 there were major developments with regard to implementation of the Personal Data Protection Act (hereinafter PDPA). The new version of the PDPA came into force on 1 January 2008.

Changing the definition of personal data and expanding on sensitive personal data by using biometric data could be considered as the most important outlets of the new PDPA. As well as increased protection for personal data processing, i.e. changes to regulations regarding the processing of personal data provided for legal public use, regulations on processing personal data for the purposes of research or government statistics and setting up the DPO (according to the Directive 95/46: Data Protection Official) institution responsible for personal data protection.

Since January 2008, the category of private personal data no longer exists. With the new version of PDPA the personal data are divided into sensitive personal data and personal data. With invalidating the private personal data category, the duty of notifying the processing of private personal data was also cancelled.

As mentioned before, biometric data, especially fingerprint images, palm print and iris images, are handled as sensitive personal data, and data relating to genetic information was replaced by the term "genetic data".

Furthermore, a new provision on the disclosure of data was put forward. From January 2008, a person has a right to request that his/her personal data, lawfully designated for public use, no longer be disclosed or used. Therefore, a person retains control over further usage of this data after its disclosure, which the previous wording of the PDPA did not allow.

Also, the new version of PDPA regulates the collection of personal data for solvency assessment – the data about personal payment default can be processed and communicated to third persons only within three years of the violation of obligations. Therefore, the data in the Estonian Credit Register cannot be more than three years old, and older data must be removed. Basically, the goal of this amendment was to ensure that each processor was clear about the basis for processing the data and ensured that contracts, agreements and other documents were not contrary to the requirements of the law.

The requirements regarding the consent of the data subject were also changed. A person can prohibit the processing of such data for which the legal basis for disclosure and processing cannot be verified. In cases where the initial data processing was carried out for journalistic purposes (there are new relevant provisions in the law) or on the basis of law (for example, databases accessible to the state public), the further data processing cannot be prohibited.

B. Major case law

The processing of personal data for journalistic purposes without the consent of data subject
The new version of the PDPA, which came into the force on 1 January 2008, brought changes to the provisions on processing personal data for journalistic purposes and making audio or visual recordings in a public place.

Unfortunately, the first negative experiences on this sensitive matter have occurred. For example, in 2008 the Estonian Data Protection Inspectorate (hereinafter EDPI) initiated misdemeanour procedure based on a complaint from a private person appearing on a TV channel. According to the complaint the filming team of the TV channel videotaped the private person and his farmhouse on the territory of his farm without asking for the person's permission and without the consent of the person. The report was broadcasted in the popular news programme of the TV channel, even though the person prohibited it.

The processing of personal data is allowed only with the consent of the data subject and it must clearly establish the amount of data for which the permission for processing is given, the purpose of processing the data and the persons to whom transmission of the

data is permitted. Silence or inaction is not deemed as consent.

In this case, the assumption that the person was informed about the visit of the filming team cannot be counted as that person's consent. Thus, the filming team started videotaping without the consent of the person. In addition, no consent was requested to broadcast the report in the news programme.

The exemption in the new version of the PDPA stipulates that personal data can be processed and disclosed in the media for journalistic purposes without the consent of the data subject, if there is predominant public interest and this is in accordance with the principles of journalism ethics. In this case the public interest was not clarified, thus the exemption was not taken into the consideration.

The TV channel was punished for filming and broadcasting the report without the consent of person with a fine €760.

C. Major specific issues

For the second year, on its own initiative, the EDPI formulated the supervisory priorities for the year. There were several topics chosen that were dealt with in depth at this time, and an opinion or instructive document was published with regard to these on the EDPI website (http://www.aki.ee). The topics were selected by the officials of the EDPI and were considered as the most problematic issues in the area of personal data protection and freedom of information.

On the basis of the topics, analysis and any necessary on-site supervision were conducted, and the guidelines/ guidance documents were prepared as a result.

The priorities chosen and the guidelines issued in the accounting period were the following: processing of personal data of the sponsors of the political parties, processing of personal data by the accommodation providers, processing of passengers' personal data, taking photos in the educational institution, registering the processing of sensitive personal data by security firms, publishing lists of students and graduates. Additionally, the EDPI composed a self-evaluation questionnaire for the data processors with the purpose of clarifying and analysing the data processing system and procedures within the company.

Finland

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

The Directive of the European Parliament, and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which came 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 came 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 respect, 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.

Amendments

During the year under review, there were no actual amendments to the Personal Data Act (523/1999) but provisions pertaining to personal credit data were extracted from it to form an Act in its own right. The transition period of the Credit Data Act ended on 1 November 2008. In part, the Act provides data protection also to legal persons and specifically requires that the data controllers have sufficient data protection competence at their disposal. A new chapter, 5a, was included in the Act on Protection of Privacy in Working Life, which provides detailed provisions on the use of personal credit data in working life.

During the year under review, the amendments required by the directive (2006/24/EC) were entered in the Act on the Protection of Privacy in Electronic Communications (516/2004). The deadline for their implementation is 15 March 2009.

In 2006, the Finnish Parliament instructed the Government to begin preparation of legislation on the general protection of personal data in biometric identification. According to the Ministry of Justice, which is responsible for preparing the Act, the general provisions on the processing of biometric identification will be prepared in conjunction with the general review of the Personal Data Act (95/46/EC Article 8, paragraph 7) to be commenced later.

B. Major case law

On 17 July 2008, the European Court of Human Rights gave its ruling in the matter of I v. Finland (No 20511/03). The matter pertained, among other things, to a person's right to find out, on the basis of log data, who has had access to their patient records. Finnish legislation requires that data protection be provided in part to specifically ensure that access to this kind of information can be ensured. However, the data system of the hospital was implemented in such a way that the administration of access rights and the log file could not indicate in detail the persons who had processed data on them. As a result, and applying the principle of obligatory prosecution, the criminal court could not convict any one person of a crime. In its ruling, the European Court of Human Rights said that a situation has occurred, caused

by the functional characteristics of a data system that was not controlled as provided in the law, in which the protection of the personal life of the person in question as enacted in Article 8 of the European Convention on Human Rights has been violated. The decision is particularly significant because the European Court of Human Rights applied the Convention on Human Rights to an electronic data system and its deficiencies.

The Court of Justice of the European Communities (the Grand Chamber) gave its ruling on the publication of data on earned income on 16 December 2008. The matter pertained to the scope of application of Directive 95/46/EC, the processing and mobility of personal data on taxation, protection of individuals and freedom of speech. The Court left the journalistic processing as referred to in Article 9 of Directive 95/46/EC to be determined by a national court. On the other hand, according to the ruling, the Data Protection Directive must be applied to the processing of personal data derived from public data sources and the use of previously published lists or services. The matter is still being processed in the Supreme Administrative Court in Finland.

The competent Data Protection Board gave its decision on the matter initiated by the Office of the Data Protection Ombudsman on the authentication of quick loan applicants via mobile phone. In its decision, the Data Protection Board ruled that the practice whereby the creditor identifies the loan applicants solely on the basis of the name, social security number, address and telephone number data provided via a text message that is accepted as a loan application, cannot be considered as a sufficiently reliable practice. Therefore, the Board prohibited the respondent, who followed an authentication process commonly used in the sector, from processing personal data in the aforementioned manner. The respondent lodged a complaint against the decision of the Data Protection Board to the relevant appeal court. Partly due to this case, a proposal to enact a general law on authentication was put forward in Finland.

C. Major specific issues

Attention to special laws

According to Section 10 of the Finnish Constitution, personal data protection must be enacted in law. Due to this provision, there are currently up to 650 special laws legislating on the protection of personal data. With regard to the transfer of data between authorities, the general law to be applied alongside the Data Protection Act is the Act on the Openness of Government Activities.

The tragic school shootings in Jokela and Kauhajoki highlighted the issue of the workings of the whole legislative framework. Particular attention was paid to legislation on student welfare, firearms and healthcare. It was established that the authorities in various administrative sectors had not paid sufficient attention to the state of legislation. On the other hand, it was easy to observe that personnel who had to apply legislation at the local level had not received sufficient information and guidance. Therefore, in problem situations, they were unable to act within even the permitted limits of legislation.

Surveys conducted

During the year under review, the Office of the Data Protection Ombudsman conducted several surveys. The national Act on the electronic processing of client data within social welfare and healthcare entails a specific provision to appoint a person responsible for data protection in each unit. In addition, the Act requires that the manager of each unit draws up specific, applicable data protection guidelines. According to our survey, the implementation of the provisions started off well but the situation could still be improved. At the same time, wide-ranging education for persons responsible for data protection was launched, which at its most comprehensive is university level.

In the so-called web police survey, we analysed the legality of processing personal data in Finnish web-based services. The survey focused, for example, on services providing social networking, services for children and young people and services collecting sensitive personal data. The results of the survey showed that a great deal remains to be done with regard to the fulfilment of the

information obligation. Special measures were applied to some of the service providers surveyed.

Our third survey assessed the functioning of the Personal Data Act and partly the criminal sanction system. In our survey, we analysed, among other things, the sentences passed by courts and decisions made by prosecutors.

The survey showed that the number of data protection offences continues its slow but steady increase, which is thought to be caused by the improved communication on the rights for and significance of data protection, increasingly secure data systems, and the improved professional competence of the police and prosecutors. On the other hand, there was some discussion on whether the sanction system is strict enough.

Scientific research

Scientific research often deals with sensitive personal data. For research purposes, data is often needed from a variety of sources. In our experience, researchers are often very insufficiently informed on the requirements set by data protection on scientific research. For this reason, we implemented an extensive and comprehensive web-based guidelines project in cooperation with various authorities. The aim of the project was to improve the level of data protection in scientific research, to make researchers' work easier and improve the practices of authorities functioning as sources of information. The project output includes virtual guidelines together with their requisite quality assurance systems and several manuals determining best practices.

France

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

France has transposed the European Directive of 24 October 1995 in the Act of 6 August 2004 amending the Act of 6 January 1978. A first implementing decree was adopted on 20 October 2005 and was amended on 25 March 2007 in order to incorporate the necessary procedural changes.

B. Case law

The Council of State Order of 19 February 2008 establishes the judicial role of the CNIL

Since the law of 6 August 2004, the National Commission for Information Technology and Civil Liberties, the CNIL, has a sanctions unit with the authority to initiate proceedings and impose sanctions against those responsible for processing data. The nature and status of this judging unit were specified by the Council of State in a decision of 19 February 2008. Indeed, the Council of State considered that the "limited bench" of the CNIL should be classified as a "jurisdiction", in the sense of Article 6(1) of the European Convention on Human Rights and Fundamental Freedoms. This decision is important and demonstrates that, in addition to its role as guardian of public liberties, the CNIL has established itself as the regulatory authority, thus ensuring the effectiveness of each person's right to protect their personal data.

C. Major specific issues

Adoption of resolutions

During 2008, the CNIL has been in session 50 times for 36 plenary sessions and 14 dispute sessions. These meetings have led to the adoption of **586** resolutions, an increase of **50 %** compared to 2007.

The CNIL adopted in 2008:

- **391** authorisations (**+84 %** compared to 2007);
- **18** authorisation denials;
- **29** recommendations on processing sensitive or high-risk data.

Referrals

The CNIL received 6,760 referrals in 2008

In 2008, 4,244 complaints and 2,516 applications for indirect access rights were referred to the CNIL (a slightly lower number (-5 %) compared with 2007 (2,660 applications), but still a significant increase (+58 %) compared with 2006 when there were 1595 applications).

Although the volume of complaints was also just slightly down, this confirms the very high expectations of citizens in terms of respecting freedoms.

File notifications also changed considerably in 2008, rising to 71,990 compared with 56,404 in 2007, an increase of around **27 %**.

Inspections

In 2008, **218 inspections** were conducted, **an increase of 33 %** compared to the previous year. In the early 2000s, there were never more than around thirty inspections. It is worth noting that opposing a CNIL inspection constitutes an offence punishable by one year's imprisonment and a fine of 15,000 euros. In this respect, the first conviction for a "crime of obstruction" was issued by the Paris District Court in January 2009, following two oppositions to inspections in February and April 2008.

The conditions of the application of the French Data Protection Act have been inspected within **145 organisations.**

The inspections conducted by the Commission are undertaken in order to enable **implementation of the annual programme** adopted by the CNIL, which define the themes prioritised by the commissioners.

In this context, **the topic of electronic voting** has been central. Twenty inspections were undertaken of electronic voting operations in the context of professional elections. The inspections assessed the secrecy of the ballot, the personal, free and anonymous nature of the voting process, the fairness of the electoral operations and the effective monitoring of the vote.

The **local authorities** sector has also been inspected due to many files they hold, for various purposes (marital status, electoral lists, social welfare, municipal police, land administration, school enrolments, etc., which can sometimes be sensitive) and the nature of the data held.

2008 was marked by **the end of the inspection of the STIC file** (Criminal Offences Processing System) managed by the Ministry of the Interior. This file gave rise to nearly twenty on-site inspections at police stations, regional criminal investigation departments, courts, prefectures and the regional directorate for general information, and allowing a very detailed analysis of their operation.

The second focus of the inspections conducted in 2008 was the performance of on-site audits parting response to complaints received by the CNIL. **25 % of the inspections carried out in 2008** took place as part of the investigation of complaints.

Penalties

Following the Act of 6 August 2004, the CNIL has had sanctioning powers, giving it the right to impose fines of up to 150,000 euros (300,000 euros in the case of repeat offences), up to a limit of 5 % of turnover.

In 2008, the CNIL imposed a total of:

- 9 pecuniary penalties consisting of fines of between 100 and 30,000 euros;
- 1 warning;
- 126 (+20%) warnings.

The Information Technology and Civil Liberties Correspondent (ITCLC)

Article 22 of the Act establishes that in the presence of a "data protection correspondent", known as the Information Technology and Civil Liberties Correspondent (ITCLC), within an organisation, the organisation is exempt from the most common reporting formalities. The corresponding records are now held in a register kept by the ITCLC. However, data processing which is deemed to be "sensitive", requiring authorisation or an opinion, continue to be submitted to the CNIL.

At 31 December 2008, **3,679** organisations had appointed an ITCLC, which is an increase of **104 %** compared to 2007. The total number of ITCLCs as of 31 December 2008 was 989, as many organisations share their Information Technology and Civil Liberties Correspondent. **89 %** of appointments were made in the private sector, with the public sector accounting for **11%.**

The ITCLC must allow the data controller to comply with its obligations, in particular the rights of people affected: the right to access, right of rectification and removal, the right to object. Thus, the role of the ITCLC is to advise the data controller so that its strategic guidelines comply with the Data Protection Act. The ITCLC should also alert the data controller in the event of shortcomings in order to avoid possible criminal penalties. Therefore, the ITCLC represents a source of legal security and reflects organisations' ethical aspirations.

Highlights of 2008

The Edvige file

In 2008, the CNIL ruled on the creation of the "Edvige" police file

In March 2008, the CNIL was requested by the Ministry of the Interior to give its opinion on a project to create a national database implemented within the framework of the reform of the French Information Service, entrusted to the Central Public Security Directorate (DCSP).

The Ministry of the Interior had not wanted the decree for the creation of the "Edvige" file[18] to be published in the Official Gazette. However, in the interest of democratic transparency and citizen information, the CNIL requested that the text be published so that a public debate could take place. This request was successful as both the Act creating the file and the corresponding notice were published.

Publication of details of the creation of this file also has the effect of allowing on-site and documentary inspection of this file by the CNIL, which constitutes an additional guarantee.

The CNIL has also ensured that the processing in question will not be subject to any interconnection, matching or any form of linkage with other files, including those of the police.

[18] Translator's note: "Edvige" is the acronym of "exploitation documentaire et valorisation de l'information générale", which translates as "documentary exploitation and utilisation of general information".

The CNIL also intervened to ensure that the recording of data on public figures, trade union members, religious figures or politicians (elected locally and nationally) is clearly defined, particularly with regard to the storage of data relating to the "behaviour" or "travel" of such figures.

The initial draft decree contained no limitation on the time limit for holding the stored data. The CNIL has worked to ensure that a period of no more than 5 years is established, for information collected on individuals who undergo an administrative investigation when applying for certain jobs (security, etc.).

The CNIL has expressed reservations about several aspects

Regarding the collection of information relating to minors, the CNIL has reiterated its commitment to the principle that such collection must remain exceptional and subject to strong safeguards. It expressed the wish that the minimum age for collecting information on minors be increased to 16 years instead of 13 years as is currently the case.

The issue of the age of persons who may be put on file must be viewed in conjunction with the lack of a time limit for the retention of data. Although minors can be responsible for "*disturbing the public order*", it does not seem legitimate that such facts could be used against them 30 years later. The right to erasure should be guaranteed for all, including the citizens of tomorrow.

The CNIL also considered that the possibility of collecting information on ethnicity, health and the sex lives of individuals was not undertaken with sufficient safeguards in place.

It also underlined that it did not have precise information about the levels of technical security around use of the "Edvige" file or the possible existence of a traceability mechanism to verify the conditions of access to data contained in the file by public authorities. This information is necessary to enable it to fully carry out its monitoring role.

Finally, the CNIL regretted the lack of a formalised procedure for the updating and clearing of files. It did note, however, the annual requirement imposed on the National Commissioner of Police to report to the CNIL on the police force's activities related to auditing, updating and deleting information stored in the "Edvige" file.

In view of these comments and the reactions to the publication of the Edvige Decree, the government withdrew the text. It asked the Commission to prepare new proposals, in particular regarding the time limit for the retention of information relating to minors and the storage requirements for certain types of sensitive data, also announcing that it would not store this file in any data relating to public figures.

The development of biometrics

The number of biometric devices referred to the CNIL for approval or recommendations is constantly growing. Since 2004, over 1,800 applications have been submitted to the CNIL, 1,500 of which are for devices implemented in accordance with the rules established by the CNIL regarding hand contour recognition or digital fingerprints.

Through its Assessment Department, the CNIL plays a role in supporting businesses during the design of their operating systems to ensure the protection of personal data. This Department has been particularly involved in development of the systems described below.

The biometric visa or VISABIO

This new biometric visa system was the subject of an experiment in 2004, within the framework of the BIODEV pilot project. VISABIO should affect over two million foreign nationals from countries subject to visa requirements every year. The aim is to enable collection and storage in a centralised database of biometric information: the scanned passport photo and the ten digital fingerprints of the applicant, along with data previously collected during the visa application procedure.

Although the use of such data undoubtedly facilitates identity checks and authentication of the identity documents produced with them, the CNIL considers that this process must take place within strictly defined limits. The CNIL particularly deplores that no attention has been paid to the possibility of only retaining the biometric data on the biometric visas, and not in a

central database. Finally, the CNIL underlined the special importance regarding the collection of fingerprints of children over 6 years of age. This fingerprinting should not be regarded as a simple technical measure, but requires thorough debate.

The biometric passport
In 2007, the CNIL expressed its opinion on the draft decree. The decree, the practical implementation of which is due to take place by 28 June 2009, provides for the issue of passports with an electronic device containing not only a scanned passport photograph, but also two digital fingerprints, in accordance with the Council of the European Union regulation of 13 December 2004.

The decree also provides for storage in the Delphine file of the scanned photographic identification of the passport applicant as well as eight of his digital fingerprints. This data storage gives rise to significant changes in the database.

The CNIL has expressed reservations raised by this project since it gives rise to the creation of the first biometric database of French nationals for administrative purposes. It particularly stressed that the automated and centralised processing of this data is acceptable only insofar as it is justified by considerations linked to public order or national security. On this point, the CNIL considers that the arguments put forward to justify the creation of such a database - the improvement of procedures for issuing or renewing passports or, more generally, the fight against fraud – are not entirely convincing.

Indeed, the storage of scanned identity photographs and fingerprints in a centralised database seems disproportionate to the objectives stated. Given the reservations of the CNIL, the Interior Minister has agreed that scanned fingerprint may not be used for identification purposes and that no recognition device may be operated using the database of scanned identity photographs.

The CNIL has also raised concerns that the new procedure for issuing passports is being adopted by means of a regulation, and not via the legislative route, as the changes being introduced go beyond the measures advocated by the European Union. The scope of this reform and the important underlying issues undoubtedly warrant a public debate and the drafting of a bill.

Voice and vein pattern recognition
In 2008, the CNIL authorised, for the first time, the use of devices based on voice recognition and the vein pattern of the finger. These licences have been adopted following thorough technical assessments. The CNIL has ensured that these devices do not pose risks in terms of data protection.

Voice recognition
The voice recognition system aims to secure and facilitate the management of passwords used to access the information system of, in this case, the company Michelin. The process implemented makes it possible to automatically generate and reset passwords. It is based on recognition of the voiceprint, which is digitised and then segmented into sampled units. During the induction process, each employee will record the pattern of his voiceprint. When he wishes to renew his password, he must call a specific automatic calling machine. The system then performs a comparison between the words repeated by the user and the reference profile.

During this assessment, the Commission ensured that staff had adequate information and that full measures were taken to guarantee security of the data and prevent any risk of identity theft.

Vein pattern recognition
The CNIL has also authorised, for the first time in 2008, the implementation of five devices based on the recognition of the vein pattern of finger, for the purpose of controlling access to premises or to information systems. This technology is a serious competitor to the now conventional technology (fingerprints, iris scans, hand contour, etc.). It is based on the recognition of the intertwining of blood vessels. This method has the advantage of recognising a pattern hidden beneath the skin, so it is not possible, at least currently, to capture and copy this biometric information without the knowledge of the person concerned.

Following a technical assessment, the CNIL considered that the vein pattern, in the current state of the technique,

is an untraceable form of biometric information whose storage in a database presents fewer risks than the digital fingerprint.

Video-surveillance

Over the past five years, the CNIL has recorded an increasing number of video-surveillance notifications. In 2008 alone, 2,588 notifications were made, compared to 1,317 in 2007.

The number of complaints has also increased sharply in recent years, totalling **173** this year (an **increase of 43 %**). In line with its role, the CNIL conducted several on-site inspections and issued many warnings to organisations that installed video-surveillance systems that did not comply with the formalities prescribed by law.

The considerable importance that video-surveillance is acquiring calls for a clarification of the legislation applicable to it.

A complex legal framework, a source of legal uncertainty

Currently, video-surveillance systems can come under two different legal systems:

- **the law of 21 January 1995**, which makes video-surveillance systems that cover places open to the public subject to authorisation from the prefecture;
- **the Data Protection Act of 6 January 1978**, amended in 2004, which regulates video-surveillance systems installed in places which are not open to the public, such an businesses, or systems located in public places when they are coupled with a biometric technology (facial recognition, for example).

In practice, this legal framework, which allows the coexistence of two different systems, lacks clarity. Its implementation is complex since the majority of video-surveillance devices now use digital systems, which process personal data in an automated way and therefore fall within the remit of the CNIL, regardless of where they are installed. In view of this situation, the CNIL considers it necessary to quickly clarify the current video-surveillance system in order to better regulate practices.

The issue of the control of video-surveillance devices by a truly independent body is fundamental in modern democratic societies.

The introduction of video-surveillance systems requires real public support. While some opinion polls show that people are generally supportive of video-surveillance, the French are not willing to forego protection of their individual rights.

To aid its analysis of the issue, the CNIL entrusted the IPSOS with **the task of conducting a study of French public opinion regarding video-surveillance**. The study conducted in March 2008 among a sample of 972 people, representing the French population aged 18 and over, confirms that a large majority of French people (71 %) are in favour of the presence of CCTV cameras in public places. 65 % of them believe that more cameras will help the fight against crime and terrorism.

The idea of placing these video-surveillance devices under the control of an independent body appealed to a large majority of French people (79 %), who consider the CNIL to be the most appropriate body to perform this control.

It is only by having both a video-surveillance system that functions within a framework of clear legislation for the protection of individual rights, and an independent monitoring body, that we can talk of "video protection" in the sense given by the Interior Minister.

Germany

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

Act on the implementation of the IPR Enforcement Directive

On 11 April 2008 the German Bundestag adopted the Act on the implementation of the IPR Enforcement Directive (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights), which came into force on 1 September 2008 (Federal Law Gazette I 2008, 1191). It provides for an amendment of several acts on the protection of intellectual property rights:

The Patent Act, Utility Model Act, Trademark Act, Act on the Protection of Semiconductors, Copyright Act, Registered Designs Act, Plant Varieties Protection Act, were to a large extent amended by using identical wording. In particular, it grants the rights owners, above all the music and film business with a view to "piracy" in file sharing places on the Internet, a right to information in the area of civil law against Internet access providers in order to find persons potentially breaking the law. However, a judicial order is required to provide information, which, from a data protection point of view, is indispensable with regard to using traffic data to provide information.

It is not permitted to use data retained for later use for the provision of information. When implementing the Directive on Data Retention, the legislator restricted the use of retained data explicitly to the purposes of criminal prosecution and to eliminating danger, Section 113b, paragraph 1, sentence 1 Telecommunications Act.

The issue of the admissibility of finding out IP addresses, which are required in order to identify the user, still remains to be settled. Identification can ensue for example by means of spy files pretending to contain the connection with certain media searched for by the user of file sharing places, which in fact are only intended to find out the IP addresses of the interested person. Thus, in reality, a download of, for example, a piece of music does not take place. In other cases, file sharing places are searched by means of the checksum of data files protected by copyright. As the computer has the requested data files available in its open folder, the respective IP address will also be found. This is also a case of covert collection of IP addresses of members of file sharing places aiming at the subsequent use of the data which is not related to the purpose.

Act on the prevention of dangers posed by international terrorism

By means of the Act on the Prevention of Dangers posed by International Terrorism, which came into force for the first time on 1 January 2009 , the Federal Office of Criminal Investigation (BKA) was granted comprehensive powers for the defence against international terrorism.

This assignment of tasks to the BKA means a break in the federal architecture of security. From the beginning, in the Federal Republic of Germany, the German Police fell within the competence of the Federal States (Länder). The assignment of preventive powers to the BKA modifies this division of competence.

From a data protection point of view, one has to mention two essential critical points:

On the one hand, it is doubtful how far the powers of data collection and data processing granted to the BKA are appropriate, necessary and suitable for performing the tasks assigned to that agency. In addition to standard policing powers, the BKA gets additional special powers of investigation even including the online search of information technology systems. Given the further subsisting competence of the Federal States with regard to prevention of dangers posed by international terrorism it is questionable whether this abundance of new competences is really adequate for the few cases in which the BKA will take action itself. I take up a critical stance towards the coexisting competences of the BKA and of the Federal State police authorities also in so far as this leads to the fact that both the BKA and also the Federal States could take parallel measures of defence and by doing so, they could process personal data multiple times.

The other crucial point as regards my critical view of the Act concerns the granting of the core of private life. In recent years, the Federal Constitutional Court has

ordered the legislator in several rulings to secure the core area when it comes to covert powers of collecting data, in particular by abstaining as far as possible from the outset from intrusions into this area. In addition, this prohibition of collecting data has to be supplemented by regulations stipulating the immediate erasure of intimate information and preventing their use if, in an exceptional case, a violation of the core area has happened. In this respect, the Act on the BKA has shortcomings.

B. Major case law

Ruling of the Federal Constitutional Court on the admissibility of online searches of information technology systems

In its ruling of 27 February 2008 on online searches the Federal Constitutional Court declared covert access to information technological system only admissible under certain, strict conditions. Thus, certain facts have to indicate in an individual case that there exists an imminent threat to an overriding important legally protected interest. This includes a person's life, limb and freedom and the assets of the general public whose exposure to threats concerns the basics or the existence of the state or of persons. In addition, the legislator has to guarantee the protection of the data subjects' basic rights by appropriate measures for procedures.

At the federal level, for the first time, the power of online searches of information technology systems has been laid down as a rule in the Act on the Prevention of Dangers posed by International Terrorism by the Federal Office of Criminal Investigation (see A.)

By the previously mentioned ruling the Federal Constitutional Court has developed the new basic right to the guarantee of confidentiality and integrity of information technology systems. This basic right – such as the right to informational self-determination developed in the ruling on population census in 1983 – is a particular development of the general personal right. The new basic right protects citizens against new threats related to the use of information technology systems. Given the rapid technological progress and the changes to the circumstances of life, such systems are ubiquitous and often indispensable. The Internet as a complex network of computers is a perfect example of this development. A consequence of this use is the automated collection and processing of data about the user's behaviour and characteristics often without the data subject's knowledge. This allows the creation of extensive personal profiles. The new basic right applies to all information technology systems which can contain detailed or significant personal data. The basic right protects the confidentiality of the entitled persons to make their own decisions about their system, about its performance, functions and contents. In the event that third parties are able to access these systems without authorisation, this is already considered as a violation of the basic right – regardless of whether it is easy to access data or whether this is only possible with considerable expenditure.

Preliminary rulings by the Federal Constitutional Court on data retention legislation

On 28 October 2008, the German Federal Constitutional Court further restricted the law enforcement authorities' access to data retained due to the "Act regulating the surveillance of telecommunications and other covert investigation measures, as well as implementing EC-Directive 2006/24/EC". In March 2008 the Court had already decided that until its final decision, it is only allowed to provide the responsible authorities with retained traffic data if these data are used for the prosecution of so called serious crimes (e.g. murder, robbery, and blackmailing) as listed in Section 100a of the Federal Code of Criminal Procedure. Since several Federal States introduced legislation within the last year allowing state intelligence as well as civil protection agencies to access the retained data in the area of prevention of danger, in its ruling of October, the court extended the restriction of the possibilities of use to these authorities.

The Administrative Court of Berlin exempted a provider from the obligation to data retention

In a preliminary decision of 17 October 2008 the Administrative Court of Berlin forbid the Regulatory Authority (Federal Network Agency, Bundesnetzagentur) from fining, as per the legal means, a provider who refused to comply with the mandatory data retention. By way of a reason for its decision, the court stated that with regard to the investments the telecommunications providers have to make in order

to assure the technological and personnel means necessary for data retention, no sufficient rules on compensation for the costs existed. Therefore, the risk of financial damage to the provider outweighs the state's benefits of the ability to access the retained data. The provider who filed the lawsuit mainly offers his services to business clients. This makes it very much less likely that law enforcement authorities will request the company's retained data. First and foremost, the decision only affects the provider that filed the action. Several providers looking for a similar ruling have filed their own lawsuits before the court in order to be exempted from the mandatory data retention. Meanwhile the Regulatory Authority has appealed against the decision of the administrative court at the competent administrative appellate court.

Administrative Court of Wiesbaden on the Directive on Data Retention: Decision on submitting the case to the European Court of Justice

On 27 February 2009, the Administrative Court of Wiesbaden decided to submit the question as to whether the Directive on Data Retention (2006/24/EC) is compatible with European Law, to the European Court of Justice for a preliminary ruling. According to the court, data retention violates the fundamental right to data protection. The individual does not provoke the interference but can be intimidated, even when he or she is behaving within legal boundaries, by the risks of abuse and the feeling of being under surveillance. Therefore the Directive does not respect the principle of proportionality guaranteed in Article 8 ECHR. http://www.vorratsdatenspeicherung.de/content/view/301/1/lang,de/

C. Major specific issues

The year 2008 was marked by the disclosure of several severe violations of data protection. At the beginning of 2008 the media reported on the covert monitoring of employees of a major groceries discount supermarket. In spring and summer 2008, in an increasingly rapid succession, the magnitude of the illegal trading of addresses as well as bank account data was revealed. One major German telecommunications company was involved in many ways, from the monitoring of communications of top managers and works councils to fraudulent call centres and data glitches of a considerable scale. But registration offices and other public agencies were also involved.

Consequently, at the end of the year the Federal Government submitted an amendment to the Federal Data Protection Act (BDSG). According to the amendment, particularly the favour given to trade with personal data for advertising purposes is to be abolished. Now, data subjects should regularly give their consent before it is permitted to use and transfer their data for advertising purposes. Among other measures, it is also intended to introduce a data protection audit. According to this plan, a seal of approval will be awarded to companies who undergo a regime of audits and comply with stricter data protection requirements – yet to be determined. With regard to the submitted draft bill, partial applications have been made for considerable change requirements. The draft bill is currently being deliberated in the Bundestag. The outcome of the deliberations is uncertain.

On 14 January 2009, the Federal Cabinet adopted the draft bill on the strengthening of Federal information technology security (BR 62/09). This law aims to grant the Federal Office for Information Security (BSI) comprehensive powers, particularly with a view to the storage and evaluation of Internet traffic and usage data. In a resolution, the Conference of the Data Protection Commissioners of the Federation and of the Länder warned that the measures envisaged for strengthening IT-security must not be implemented at the expense of data protection.

Moreover, on 4 February 2009 the Federal Cabinet adopted the draft of an Act regarding a citizens' portal. This draft aims to grant the confidentiality, integrity and authenticity in the exchange of e-mails. Basically, the focus of citizens' portals is the creation of a secure infrastructure for e-mail communication (De-Mail) and the storage of personal data (De-Safe) which are necessary for communication between citizens and administrations, for example, in relation to documents and certificates. It is intended that only private companies should be responsible for the implementation and operation of the services. The Federal Commissioner for Data Protection and Freedom of Information (BfDI)

proposed to secure communication by means of an end-to-end encryption between the sender and the addressee. However, the storage of personal data in an electronic safe is only really secure if the data are stored encrypted and only the data subject holds the electronic key.

Greece

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

New law to reinforce the privacy of telephone calls

Following a highly publicised scandal in 2005, when it was discovered that about 200 mobile phones were being tapped and conversations intercepted, including those belonging to the Greek Prime Minister and other members of the government, a new law (Law 3674/2008) was introduced in 2008 to reinforce the privacy of telephone calls.

The new law has the following main provisions:

- Each telecommunications service provider must adopt a security policy. Each policy and its amendments/updates must be approved by the Greek Authority that provides Communication Secrecy (ADAE; this Authority is different from HDPA) and also communicated to the HDPA and the Regulatory Authority for Telecommunications and Post (EETT).
- Each provider must appoint an employee responsible for ensuring compliance and the protection of the privacy/secrecy of telecommunications. The name of this employee must be communicated to the relevant authorities.
- The telecommunication service provider has a duty to take all necessary technical and organisational measures to ensure the privacy of all communications, and to carry out regular audits of their systems and infrastructure.
- All employees of the provider must exercise confidentiality.
- All voice communications taking place by means located outside the supervision of the provider must be protected by encryption techniques.
- In cases of mobile/digital switching centres, there is an obligation to record all administrative operations on the software of each centre in security logs. These logs should be stored on properly protected media which must ensure the integrity of the logs. Any direct or indirect access to these files is strictly forbidden. More details for maintaining these logs will be established in a regulation to be issued by ADAE.
- ADAE should perform regular inspections/audits of the hardware and software infrastructure of the provider to ensure compliance with legislation.
- In the case of a security breach or risk of a security breach, the employee of the provider charged with ensuring the secrecy must notify the provider or the legal representative of the provider, the public prosecutor, the ADAE and any subscribers who may be affected. The notification should be made in writing, and where direct communication is not possible, any other convenient method may be used.
- Following the breach notification, and until the public prosecutor and the ADAE have ordered specific measures, all employees of the provider shall not disclose any information regarding the security breach or the risk of the security breach, and take appropriate measures to secure any evidence.
- As part of this new law the Greek penal code was accordingly amended. Violations of the secrecy of telephone calls, including content, traffic and location data, are considered summary offences, while the evidence obtained through these violations is not permitted before a court in criminal matters.
- Finally, a National Security Plan shall be developed to protect electronic communications (not only telephone calls) of the public sector and the providers of networks and services for electronic communications. The addressees of the Security Plan shall implement the measures within 6 months. A legislative Committee, on which the HDPA is also represented, is provided for this purpose. However, so far no initiative has been taken by the Greek Government.

Lawful Interception of electronic communications in cases of child pornography

In accordance with Law 3625/2007 the Optional Protocol to the UN Convention on the Rights of the Child on the sale of children, child prostitution and child pornography is ratified by the Greek Parliament. According to this law, Article 348A of Greek Penal Code is amended so that child pornography committed by the use of electronic systems or over the Internet is an offence.

In accordance with Law 3666/2008 (Article 2 paragraph 7a) the list of crimes, for which a lawful interception of electronic communications is permitted, is amended to include child pornography.

Directive 2006/24/EC
The legislative Committee of the Ministry of Justice has finalised a draft law incorporating Directive 2006/24/EC into national law. The Draft has not yet passed through Parliament.

B. Major case law

Decision 27/2008
The Hellenic DPA was informed via a newspaper article of CCTV systems installed in two secondary schools in the prefecture of Karditsa. The DPA considered the processing of pupils' and teachers' personal data, which was taking place in the school courtyard and the corridors, as unlawful. It was deemed that such processing did not conform to the principle of proportionality, as its purpose (security on the premises and controlled vehicle/third party access) could be achieved using less intrusive means.

Decision 30/2008
Following a complaint submitted by a data subject and a subsequent audit that was carried out by the HDPA it was confirmed that a company was providing its clients with a third party lie detector service (Layer Voice Analysis application) to detect whether the data subjects dealing with them were telling the truth. The DPA deemed that the use of the specific application during a phone conversation in order to detect whether the data subject is lying or not, and particularly without first informing the person, violates Article 4 of Law 3471/2006.

Decision 48/2008
Following a request by the National Social Insurance Institute (NSII), the HDPA delivered an opinion on the following issue. The head of the above legal entity issued 330 work contracts between individuals and the NSII. The HDPA considered that it was not against the Data Protection Law to permit access to above decision to the competent Members of Parliament, including names and addresses of the 330 persons that were selected to enter into the specific contracts as well as all the applications submitted for this purpose with the relevant documentation, in order for the Members of the Parliament to verify legitimacy of the decisions. Furthermore, it was deemed that the method by which the competent Members of the Parliament would access the relevant data should be dealt by the NSII and the Parliament. The HDPA's decision was based on the idea that the competent MP's access to the above-mentioned data is necessary for the purpose of parliamentary control, which aims to verify whether the most qualified people were selected to sign work contracts with the NSII after comparisons between selected and excluded candidates' qualifications.

Decision 50/2008
Following a request by a former Orphanage resident, the HDPA decided that the adopted adult can lawfully be provided with the personal data of his/her biological parents, kept in the adoption file, for the purpose of tracing them. This includes all the information regarding the identity of the biological parents as well as any other information that could lead to the adopted person finding his/her parents.

Decision 52/2008
The HDPA received a request from an investment bank to grant a permit for the installation and operation of a biometric system, which uses the finger imprint of the employees for access control to specific electronic applications of the bank. The HDPA decided, by a majority vote, that the particular data processing in principle is not contrary to the provisions of Law 2472/1997, as it is aimed exclusively at the access control of specific employees executing transactions of large funds. The HDPA decided that where the purpose of the processing is aimed at the secure execution of transactions and the prevention of money laundering or other illegal actions, it is lawful. The Authority also decided that the particular processing does not violate the principle of proportionality for the following reasons: a) the system in question is to be used in an environment of high security standards, for specific applications of fund transactions, and the percentage of employees that will use this system, is proportional (that is to say small) in relation to the interference that this processing will cause to the employees' personality, b) the system is proportionate to the specific bank affairs that concern mainly investment activities of shipping companies, and c) the operation of the system serves the employees themselves, as it deters the illicit use of their identity, while in the event of mistaken or mischievous transaction, ensures accountability.

Decision 66/2008

A complaint was submitted to the HDPA by a data subject against a bank for not having satisfied the right of access to his data. The HDPA decided that the controller is prohibited from announcing to the data subject that an investigation is being carried out against him, regarding legalisation of income from criminal activity, or furthermore that the information related to the conclusion of the investigation has been transmitted to the competent Committee responsible for the evaluation and investigation of the above information (Article 31 of Law 3691/08). However the restriction of the right of access of the data subject ceases if the bank does not transmit the collected data and information to the competent committee, having evaluated that the collected information is not evidence of the legalisation of income from criminal activity. Furthermore, if personal data belonging to a third person were also processed by the controller, affecting the way the data subject was handled, the specific data concerns the data subject and the data subject has the right to access this data.

Hungary

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

Directive 95/46/EC
Nothing to report.

Directive 2002/58/EC
The general rules for electronic advertising have been significantly amended. According to Act XLIII of 2008 on the criteria and limitation of Business Advertising Activity *"advertising to natural persons, as the addressee of the direct marketing activity can only be sent via electronic mail or any other equivalent tool, if the addressee has unequivocally given his express preliminary consent"* to receive such advertising. In these cases, the National Communications Authority is competent in the supervisory proceeding and entitled to decide whether the electronic communication in question is an advertisement or not, and whether the law was broken by sending it. The most important amendment is that the limitations are applicable only to advertising sent to natural persons. Data not belonging to natural persons is not given such strict protection.

B. Major case law

In 2006, a civil organisation requested that the Commissioner to start an investigation against Philip Morris Hungary Ltd. regarding the processing of personal data related to a direct marketing campaign - e.g. point collection. The collected personal data was further used to send personalised brochures providing information on tobacco products. The Commissioner requested an opinion from the Hungarian Competition Authority whether such direct marketing methods can be considered as advertising of tobacco products.

According to Section 13 (1) - (2) of Act LVIII of 1997 on Business Advertising Activity *"it is forbidden to advertise tobacco, and prohibited to indirectly advertise tobacco products"*. Based on the opinion of the Competition Authority, the Commissioner came to the conclusion that personal data shall not be collected and further used for the purpose of sending personalised brochures advertising tobacco products even with the consent of the data subject. Therefore the Commissioner advised the data processor to cease the operation and ordered, by resolution, that unlawfully processed data be blocked, deleted or destroyed.

No appeal may be made against this resolution through administrative channels, thus Philip Morris Hungary Ltd. brought a lawsuit against the resolution before the competent Court. According to the decision of the Court "as the addressee requested the information himself/herself to be sent in a closed envelope, therefore the information cannot be considered as an advertisement". Having regard to the decision of the Court the Commissioner revoked the resolution and the case was dismissed by the Court. Later on, Act XLIII of 2008 on the criteria and limitation of Business Advertising Activity came into force.

In light of the new law, the Commissioner deemed it necessary to reopen the case and examine the data processing activity. According to the new law, information sent unequivocally to the addressee is considered to be forbidden advertising of a tobacco product, therefore the collected data is further processed in a way which is incompatible with the specified, explicit and legitimate purposes. As a consequence, the Commissioner banned the processing activity by resolution. This time Philip Morris Hungary Ltd. did not appeal to the Court.

C. Major specific issues

The Commissioner issued an opinion related to a decree of the Ministry on Finance which regulates the psychological aptitude test before entering into civil service at Hungarian Tax and Financial Control Administration (APEH). According to the decree those persons who undergo psychiatric treatment, or supposedly (probably) suffer from psychiatric illness which obstructs their adaptation, integration into the entity or impairs their efficiency in influencing the activity of the entity are prevented from occupying such a post. The Commissioner pointed out that special data categories such as health data may only be processed - if not ordered by the law - on the basis of the written consent of the data subject. However the legal basis itself does not make the processing possible; other criteria should also be met, especially the purpose limitation.

The fact that a person has undergone psychiatric treatment does not necessarily mean that he/she, by occupying a post, would influence or jeopardise the lawful activity of the entity. He also stressed that one's human dignity is jeopardised if the person is prevented from occupying a post because of a probable illness. The provision of the decree in question may lead to discrimination which is clearly against the Hungarian Constitution and the provisions of Act CXXV of 2003 on the promotion of equal treatment and equal chances. He underlined that such a ministerial decree as the source of law cannot provide the legal basis for data processing; only law passed by the National Assembly is able to do so. Therefore the Commissioner asked the Minister of Finance to repeal the decree.

In another case, the Commissioner investigated the data processing activity of a multinational company using GPS systems. The GPS systems were used in the cars of the company by the employees having flexible working hours, condition for the purpose of geo-location. However, there was no difference between the data collected in and out of working hours, consequently the company was processing personal data without the consent of the data subject. The processing was also not in line with the purpose limitation principle since geo-location data were also recorded out of working hours. The Commissioner expressed in his opinion that GPS systems may transmit data only during the working hours; out of work personal data shall not be processed by the employer. To make the processing lawful employees should be given the opportunity to switch off the GPS locator when using the car for private purposes.

In October the Commissioner received the draft law regarding the set up of the Central Credit Reporting System. In his opinion, the Commissioner expressed that he is against the introduction of the so-called "positive list".

Ireland

A. Implementation of Directive 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 2008 included new regulations amending the legislation giving effect to the Directive on privacy and electronic communications (2002/58/EC) in Ireland. The new regulations increase the penalties for offences relating to unsolicited communications and ensure that the burden of proving subscriber consent lies on the defendant.

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) had not yet been transposed into Irish law by the end of 2008. A bill giving effect to the Directive is expected to be approved by Parliament in the course of 2009.

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 or enforcement action. Such amicable resolutions may, for example, involve a financial contribution by the relevant data controller to the data subject concerned or to an appropriate charity. Where necessary, enforcement powers are used – for example, when data controllers fail to respect the access rights of data subjects. In some cases, data controllers are named in case studies included in the Commissioner's Annual Report. In the course of 2008, the Commissioner was involved in Court proceedings related to the rights of data subjects under the Data Protection Acts 1988 and 2003 and under Statutory Instrument 535 of 2003 (implementing Directive 2002/58/EC in Ireland). These included:

Appeal against an order from the Commissioner to erase data
In November 2008 the Dublin Circuit Court allowed an appeal by a data controller against an Enforcement Order issued by the Commissioner under Article 10 of the Data Protection Acts 1988 and 2003 (which transposes the power of the supervisory authority to order the erasure of data set out in Article 28 of Directive 95/46/EC). The case related to certain records related to psychiatric treatment that were retained by the data controller. In accordance with Section 6A of the Data Protection Acts (which transposes Article 14 (a) of the Directive), the data subject requested the erasure of these records on the grounds of the distress caused by their retention. The request was refused by the data controller. The Commissioner concluded that the data subject had a justifiable case that was stronger than the case for retention of the records put forward by the data controller. Accordingly the Commissioner issued an order directing that the data be erased. The data controller appealed the order and the appeal was allowed.

Commissioner successfully defends an appeal against a legal notice for information
The Commissioner successfully defended a Court appeal from a newspaper against an Information Notice issued in connection with an investigation of the newspaper's failure to provide access to personal data to a data subject. The newspaper had claimed that the exemption provided in Section 22A of the Irish Data Protection Acts (which transposes Article 9 of the Directive) did not require it to provide information further to this Notice. The newspaper argued that providing such information would undermine the exemption provided by Section 22A. The Court dismissed the appeal on the basis that the exemption did not apply to the Commissioner's powers of investigation under Section 10 and Section 12 of the Data Protection Acts.

A prosecution for sending unsolicited text (SMS) messages - cooperation from the Isle of Man Data Protection Supervisor
Following complaints of unsolicited text messages, the Office launched an investigation into a company with a head office based outside of Irish jurisdiction (in the Isle of Man). However, the company had staff based in Dublin and had used technical infrastructure in Ireland to send the messages. A team from the Office gathered evidence in the course of an on-site inspection. With the assistance of the Isle of Man Data Protection Supervisor, further evidence was obtained from that

jurisdiction. A prosecution for offences under Statutory Instrument 535 of 2003 (which implements Directive 2002/58/EC in Ireland) took place in November 2008. The Court imposed fines following a guilty plea by the company concerned and an admission that there was no basis for claims that the affected mobile phone numbers were validly opted-in for receipt of marketing text messages.

A prosecution for failure to comply with the Commissioner's power of access to data

Following repeated attempts to obtain information from a State-owned company in relation to the investigation of a complaint, the Office served an Information Notice on the company requiring the company to cooperate by handing over the data that was necessary for the performance of the statutory duties of the Office. The company failed to provide the information sought within the twenty-one day limit for compliance. The Office prosecuted the company for this failure in June 2008. The company pleaded not guilty to the charge but was convicted for the offence and fined. This was the first occasion that the Office felt obliged to bring a prosecution against an entity for failure to comply with a notice issued in relation to the Commissioner's power of access to data.

C. Major specific issues

As described in last year's report, the Office undertook 'raids' on a number of companies engaged in the mobile text marketing sector in 2007. 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. Following the raids, prosecutions were brought against a number of companies. One of the companies challenged the legal basis for the prosecutions. The High Court rejected this challenge. We will now be proceeding with the prosecutions.

Italy

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

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

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

New Legislation

Transposition of Directive 2006/24/EC – The legislation on traffic data retention was amended with the DPA's contribution to transpose Directive 2006/24/EC. Currently, traffic data may be retained further with a view to law enforcement purposes for twenty-four months (telephone traffic data) and twelve months (electronic communications traffic data) – irrespective of the given offence at issue. The legislative amendments better clarified the role of the Italian DPA in this sector and introduced specific punishments in connection with the failure to comply with traffic data retention requirements (section 162-bis of the DP Code).

Simplified Requirements Applying to Security Measures and Notification – Simplified arrangements were introduced in 2008 concerning certain data protection requirements to be met by self-employed professionals and SMEs (including handicrafts); more specifically, a few provisions in the DP Code were amended to eliminate cumbersome procedures applying, in particular, to the adoption of minimum security measures. The mechanisms for notifying the Italian DPA of processing operations were also simplified further, particularly by specifying what information should be included in the notification form (in line with Article 17 of Directive 95/46/EC). Additionally, specific decisions were issued by the DPA to contribute to this simplification exercise by ensuring that individuals' rights could be upheld (see below).

Cross-Border Data Flows – A major regulatory innovation had to do with cross-border data flows to third countries. Further to a request submitted by the Italian DPA to Parliament, wording was added to the DP Code to expressly refer to the use of binding corporate rules in this respect. Accordingly, Section 44 of the DP Code now provides that data transfers to third countries are allowed if authorised by the DPA on the basis of adequate safeguards for data subjects' rights "as determined by the Garante also in connection with contractual safeguards, or else by means of rules of conduct as in force within the framework of companies all belonging to the same group."

Sanctions – Significant amendments were brought about with respect to the sanctions the Italian DPA is empowered to impose. Such amendments, which considerably expanded the powers vested in the DPA, focus mainly on administrative sanctions as the criminal punishments envisaged in the DP Code were left basically unchanged. Generally speaking, the amendments in question consisted of: a. increasing the fines applying to the individual breaches; b. introducing new categories of punishable conduct; c. introducing mechanisms to better adjust sanctions to the given circumstances according to the seriousness of the conduct, importance and/or size of the database that is affected by the violation, involvement of a large number of data subjects, and the offender's financial status.

Term of Office of the Members of Independent Supervisory Authorities – Pending enactment of a piece of legislation intended to streamline the regulations applying to independent supervisory authorities, Parliament levelled the term of office of all members/commissioners of such authorities – which was set at seven years and made non-renewable.

Cybercrime Convention – Italy ratified the Council of Europe's Cybercrime Convention of 2001. The ratification instrument did not include a general clause to be incorporated into criminal procedural rules to ensure the adequate protection of fundamental human rights, in particular of the "proportionality principle" as per

Article 15 of the Convention. This requirement had been highlighted by the Italian DPA, *inter alia* in pursuance of the Opinion rendered on the draft Convention by the Article 29 Working Party; the suggestion put forward by our DPA was that an *ad hoc* clause should be added to each legal provision regulating investigational and preparatory activities in criminal proceedings whereby any investigations and procedural steps taken by the competent judicial and/or police authority would have to take account of relevance and non-excessiveness of the data and proportionate arrangements should be made. The ratification instrument also amended the provisions on traffic data (Section 132 of the DP Code) by enabling police authorities, under specific circumstances, to order IT and/or Internet service providers and operators to retain and protect Internet traffic data – except for contents data – for no longer than ninety days, in order to carry out pre-trial investigations or else with a view to the detection and suppression of specific offences. The order issued by police authorities must be notified to and validated by the competent public prosecutor.

Use of Telephone Subscriber Directories for Promotional Purposes **–** A governmental decree introduced a temporary derogation from the legislation in force on telephone subscriber directories, whereby processing of the data contained in such directories for advertising and/or marketing purposes is only allowed with the data subjects' free, prior, informed, and specific consent. This derogation was received unfavourably by the Italian DPA as it impinges on the safeguards for data subjects that had been shaped, *inter alia*, via measures and provisions issued by our Authority. The new provisions allow the personal data contained in databases set up from public telephone subscriber directories compiled prior to 1 August 2005 to be used lawfully for promotional purposes until 31 December 2009 exclusively by such data controllers as said databases were set up prior to 1 August 2005.

Video Surveillance in commonhold property – The Italian DPA drew Parliament's and the Government's attention to the advisability of enacting legislation to regulate certain issues in connection with the processing of personal data resulting from the deployment of video surveillance equipment in condos (joint tenure apartment houses). More specifically, the DPA was in favour of regulating the decision-making process in view of the installation of video cameras in a condo along with the number of tenants' votes required to approve the relevant resolution.

Parliamentary Hearings **-** The DPA was heard several times in 2008 on major issues addressed by the competent parliamentary committees either within the framework of fact-finding initiatives or in the course of the debate leading to the adoption of bills that impacted on personal data protection. In particular, the authority was heard on issues dealt with by the Justice Committee at the Chamber of Deputies (Lower House), in the context of a hearing on the governmental bill to reform the legislation on interception of communications. The DPA also contributed to the issues arising from the processing of and access to taxpayers' registry data, during a hearing held before the competent bicameral Committee. Reference can be also made to two informal hearings on issues related to the insurance sector and on bills concerning introduction of a fraud prevention system in the consumer credit sector, respectively.

B. Major case law

Criminal Liability Vested in a Journalist Publishing Information on a Child's Health. Italy's Court of Cassation (last-instance judicial authority) ruled that a journalist and the executive manager of a weekly publication were criminally liable for publishing information on the health of a well-known anchorman's baby girl. More specifically, the Court of Cassation applied the criminal measures provided for in case of unlawful processing in breach of the "Journalists' Code of Practice" that is annexed to the DP Code. This decision confirmed the peculiar legal status of said code of practice, since under Italy's DP law compliance with the applicable DP code of practice is a prerequisite for the processing of personal data to be lawful.

Precautionary Seizure of Privacy-Infringing Pictures is Lawful. The Court of Cassation ruled that a court had lawfully ordered precautionary seizure of pictures and negatives kept at the editorial offices of a newspaper (Decision No 17408/2008), in which a well-known politician was shown in the park of his villa. This issue had been previously raised before the Italian DPA,

which had found that privacy legislation had been violated following publication of pictures taken with intrusive methods and had accordingly prohibited them from being published further. The Court of Cassation ruled that the seizure subsequently ordered by a court against another newspaper that had re-published the pictures in spite of the prohibition issued by the Italian DPA was lawful. The Court found that the data subject's privacy had been violated – in line with the considerations made by the Italian DPA – because the pictures in question showed the politician's private life against his will and at his premises and had been taken in a privacy-intrusive manner with the help of specific technical equipment.

Bankruptcy Proceedings and Judicial Records. The Court of Cassation ruled that – in pursuance of legislation recently enacted on bankruptcy proceedings (Decree No 5/2006) – any reference to the bankruptcy declaration should be erased from the certificates issued by the judicial records office at the data subject's (i.e. the bankrupt's) request, upon conclusion of the bankruptcy/winding up proceeding, given that the decree in question had expressly repealed the provisions on discharge of bankrupts (Decision No 40675/2008).

C. Major specific issues

Ensuring Security of Public and Private Databases

Processing of traffic data by telephone and Internet service providers: The Italian DPA adopted a general provision (dated 17 January 2008), pursuant to Section 132 of the Italian Privacy Code, regarding the storage and processing of traffic data generated by telephone and Internet service providers. This was aimed at ensuring enhanced security with respect to 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, a deep audit of 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.

Without prejudice to the regulatory amendments described above, telecom operators will have to implement said measures by 30 April 2009.

This extension was granted by the Italian DPA also as a consequence of the requests made in July by the trade associations of providers of electronic communications services, which had applied for a longer time span to fully implement the complex security measures in question.

System Administrators: The Italian DPA considered it is necessary to undertake a specific action addressing the so-called "system administrators" to highlight their importance in relation to the processing of personal data and to raise the awareness of both data controllers and the public at large as to the sensitivity of the tasks they discharge. In the course of the inspections carried out by the Italian DPA over the past few years, it could be appreciated that most companies and major public and private organisations placed considerable importance on system administrators, but that this was not always the case – with the resulting risk of underestimating the consequences resulting from the unsupervised activities of administrators, who are also supposed to monitor and control the appropriate use of IT systems. Accordingly, all the controllers of processing operations that are performed, in whole or in part, with the help of electronic tools were called upon to take due account of the need to consider the risks and criticalities related to committing the tasks of system administrators. At the same time, an initial set of organisational measures were laid down to enhance awareness among public

and private bodies and organisations of the existence of certain technical functions, of the responsibilities vested in such functions and, in some cases, of the identity of the individuals working as system administrators in connection with the various services and databases at issue. Such measures include, in particular, the need for carefully assessing personal qualifications of candidates; appointing system administrators individually; keeping a list of the existing system administrators (in particular whenever human resource data are handled) and providing the relevant information to data subjects and staff alike; ensuring that systems are in place to log access (via computer authentication) to processing systems and electronic databases as performed by system administrators.

Tax Data and Privacy

Dissemination of Tax Returns Data via the Internet by Italy's Revenue Office: The Italian DPA prohibited the Italian Revenue Office from posting the tax returns of all Italians on the Internet a few days after the data had been made public on the Revenue Office's website. Dissemination of the data was found to be in breach of the sector-specific legislation, which allowed for different, less privacy-intrusive mechanisms to obtain information on taxpayers' income. Posting of the data on the Internet was also found to be disproportionate vis-à-vis the purpose of making available the information in question.

The consequences resulting from this blanket, unfiltered disclosure of the data concerning all Italian taxpayers were manifold. A considerable number of users in Italy as well as abroad were able to access a huge amount of data in the space of a few hours, since the data were available at a single source; they could copy the data, generate their own databases, modify and/or process the data, create profiling lists, and circulate the data further with all the attending accuracy risks.

In addition, it could be established that the Revenue Office had failed to request the Italian DPA's opinion – which is mandatory under the law – prior to adopting the decision to publish the data on the Internet.

Taxpayers' Register: A decision adopted in September 2008 took stock of the criticalities found by the Italian DPA following several inspections that had been carried out with respect to the taxpayers' register – where millions of records on Italian taxpayers are kept and may be accessed, via different tools, by a considerable number of users including public and private bodies – and set forth the technological and organisational measures required to enhance security of access and bring the processing into line with data protection legislation. Given that the main criticalities in question were related to the lack of information on the overall number of access-enabled users, poor monitoring of access and inappropriate use of passwords and user IDs, and the inadequate technological measures to ensure data security, the Italian DPA required regular monitoring of the access-enabled bodies and organisations; carrying out a survey of all data flows from and to the Register including the particulars of the entities able to access the Register, the applicable legal grounds, nature and type of the transferred data; partitioning the data that may be accessed to ensure that only such data may be viewed as the individual user is authorised to access; implementing alert systems to detect and prevent security breaches; implementing authentication/enhanced authentication mechanisms; logging access and restricting the maximum number of instances of access; implementing secure connection channels in case of web-based data-flow management; timely disabling of users no longer entitled to access the relevant data.

Simplification Measures

As already pointed out, the simplification exercise with respect to certain data protection requirements continued throughout 2008 with the contribution of the Italian DPA. Practical arrangements were laid down in a decision issued at the beginning of the year to further facilitate standard management and accounting tasks in both the public and the private sector, especially whenever no sensitive or judicial data are processed. To that end, simplified mechanisms were laid down with respect to information obligations vis-à-vis data subjects, without jeopardising the scope of the protection afforded by law. Additionally, data controllers were urged not to request the data subjects' consent if they only process personal data for standard management and/or accounting purposes, also in connection with fulfilling contractual, pre-contractual and/or regulatory obligations. In pursuance of the balancing of interests

principle as well as in accordance with specific conditions, the DPA ruled that data controllers in the private sector were allowed to use the mail address information provided by a data subject they had delivered a product and/or a service to without that data subject's consent, if they pursued standard management and/or accounting purposes and the mailing was intended to directly send their own advertising and/or direct selling materials or else carry out their own market surveys and/or provide commercial communications. In yet another decision, the Italian DPA laid down simplified arrangements to implement minimum security measures with respect to certain data processing categories. This was aimed – in line with the provisions already laid down in simplification-oriented legislation (see above) – at affording an adequate security level by taking account of the features applying to small-sized businesses and the processing operations that are only aimed at accounting and/or management purposes.

Healthcare and Sensitive Data

Guidelines for Data Processing within the Framework of Clinical Drug Trials: These Guidelines were issued in 2008 to lay down the safeguards data controllers are required to provide when processing personal data related to patients undergoing clinical drug trials; a public consultation was subsequently launched concerning these Guidelines. The guidelines require, in particular, that data and biological samples should be retained for a shorter period; that more clear-cut distinctions should be drawn between consent to medical treatment and consent to the processing of personal data; that a specific clause be worded to obtain the patients' consent so as to enable data subjects to have their voice heard also with respect to any processing operations performed by other entities that collaborate in the given research, perhaps from abroad; and that more stringent security measures should be adopted. The DPA also drafted a model information notice that could be used by the pharmaceutical companies sponsoring the studies to inform patients on the processing of their data via the testing centres involved. Security measures were upgraded particularly in relation to electronic data transfers; mandatory data access authentication procedures were laid down along with the use of data storage and archiving systems based on encryption and secure communication protocols to transfer data between testing centres, the pharmaceutical company's database, and study monitors.

Anti-Doping: Further to a report lodged by the Italian Professional Bikers' Association (ACCPI) complaining to the Italian DPA that the regulations applied by Italy's CONI (National Olympic Committee) to perform anti-doping controls in non-competition periods were in breach of Italy's privacy legislation, the Italian DPA issued a decision regarding the processing of personal data in the field of anti-doping. The DPA stressed that the processing of personal data by CONI (which is a public body) must comply with all the applicable legislation and take account of relevant international instruments. The DPA ordered CONI to amend the notice used to inform data subjects (athletes) so as to provide specific information on the data to be made available, by specifying whether this is to be done on a mandatory or optional basis and what consequences arise from the failure to make available such data, with particular regard to the detailed information on location. In addition, the scope of communication of the data in question had to be clarified by specifying (the categories of) recipients and whether the data would be transferred abroad.

Justice

The work aimed at ensuring respect for data protection principles in connection with justice-related activities continued in 2008. Within this framework, the DPA adopted "Guidelines on Data Processing by Court-Appointed Experts", which clarify the obligations these professionals must respect in handling the major amount of personal data they process in relation to different judicial proceedings. The "Code of Practice Applying to Defence Investigations by Legal Counsel and Private Detectives" was also adopted in 2008. This Code sets forth the safeguards legal counsel and private detectives should abide by when processing their clients' personal data – from the initial steps taken in preparation for bringing an action until the after-trial phase. More specifically, this Code lays down simplified arrangements with respect to information notices, stringent technical and organisational measures to protect the data, and a limited retention period applicable to the information collected for said purposes.

Business Information

The DPA issued a decision regarding the data processing carried out by a company managing own databases that are generated by extracting information from other filing systems (whether set up by public or private entities) to provide their customers – mostly business professionals and practitioners such as banks, finance companies, information companies and agencies – with information-related services focused on so-called business information with respect to given target entities (other companies, professionals, etc.). By a decision dated 30 October 2008, the DPA ordered the company to take any and all measures that were necessary as well as appropriate to safeguard data subjects in order to: a. prevent information that cannot be related directly to the given data subject, as it has to do with events concerning other entities, from being linked up with the said data subject; b. draw a distinction between the cases where, based on the available elements, no prejudicial items are found to relate to the target entity and the cases where the business reliability rate is set to "low". Additionally, the DPA prohibited the company: a. from using information that is irrelevant and in any case not directly related to the target entities; b. from providing their customers with data related to the number of queries performed with respect to the dossier on a given target entity; c. from processing the data taken from electoral rolls in order to perform consistency checks when providing their services; d. from processing the personal data related to taxpayers' returns as submitted for 2005 and stored following their publication by Italy's Revenue Office (see above paragraphs). The company was also ordered to erase said data without delay.

Electronic communications

Electrical and Electronic Waste and Data Protection: By a decision dated 13 October 2008, the Garante drew the attention of legal persons, public administrative bodies, any other bodies and natural persons that do not destroy, but rather dispose of devices containing personal data after using them in discharging the respective tasks, to the need for making suitable arrangements and taking suitable measures, also with the help of third parties with the appropriate technical skills, in order to prevent unauthorised accesses to the personal data stored in the electrical and electronic equipment. Whoever plans to reuse and/or recycle waste electrical and electronic equipment or components thereof must make sure that no personal data is present and/or intelligible in said equipment and obtain, where feasible, an authorisation to erase such data and/or make them unintelligible.

Itemised Billing: By a decision dated 13 March 2008, the Garante authorised all the providers of publicly available electronic communications services under Section 124(5) of the Code to display the full numbers of communications in the itemised bills requested by their customers as from 1 July 2008, on the condition that they enabled their users to perform communications and request services from any terminal by availing themselves of payment methods other than billing, and on the condition that they provided all their subscribers with appropriate information notices to be included in at least two bills and posted on the providers' web sites.

Telephone Marketing: Following several claims and reports related to unsolicited phone calls performed by and/or on behalf of several telephone operators and/or companies marketing goods and services, the Italian DPA prohibited several companies specialising in developing and selling databases from further processing the personal data (i.e. the phone numbers) relating to millions of users. The phone numbers at issue had been collected and used unlawfully, since no prior information had been given to data subjects who had not consented specifically to the transfer of their data to other companies.

This prohibition also applied to other companies that had purchased the databases from the companies in question in order to contact users and market their products and services via call centres. The prohibition orders followed several warnings and inspections by the DPA; the inspections had been carried out at the premises of the companies that had created and sold the databases, with respect to the telephone operators and companies that had purchased those databases, and at the call centres that had contacted the users in question.

Of note, one of the companies offered, on its website, the data of over 15 million Italian families grouped by income and lifestyle without informing the data subjects and obtaining their consent to communicate their data to third parties.

It should be recalled here that a recent legislative amendment (see Part 1) provided for an exemption from the above rules on subscriber consent, whereupon the personal data contained in databases set up from public telephone subscriber directories compiled prior to 1 August 2005 may be used lawfully for promotional purposes until 31 December 2009 exclusively by such data controllers as said databases were set up prior to 1 August 2005.

Location Data and "Check Boxes" Installed on Coaches: In a decision issued upon completion of prior checking activities, the Italian DPA authorised the processing of location data by local public transportation services. The Italian DPA also authorised processing of additional information related to the "driving pattern" and a few parameters (e.g. brake oil pressure at start and end of braking, vehicle speed during braking, etc.) as collected at the time of accidents via an "event data recorder".

The Italian DPA authorised the processing operations in question upon compliance with a set of requirements: data subjects (drivers) should be provided with detailed explanations on the nature of the processed data and the features of the system relating to the different purposes to be achieved; access to the processed data should only be allowed to persons that had been entrusted therewith by the company and were lawfully entitled to access the data on account of their tasks; the data should be kept for no longer than necessary to achieve the purposes in question – by anonymising, as appropriate, location information and processing such information exclusively as aggregate data with a view to monitoring and planning the public transportation service. As for "driving pattern" data, which would be processed in order to grant bonuses to the employees that adjust their driving patterns to corporate standards, the processing should take place in accordance with the applicable legal restrictions – in particular those set forth in section 10 of EC Regulation No 561/2006 of 15 March 2006. The procedures to be put in place pursuant to section 4(2) of Act No 300/1970 – whereby the agreement of trade unions must be obtained and/or a provision by the local agencies of the Ministry for Labour is required to monitor employees remotely – should be complied with beforehand. The company will have to notify the processing to the Italian DPA as regards, in particular, location data, and also appoint the service provider as data processor under the terms of Section 29 of the DP Code.

Formal Complaints

Online Newspaper Archives: The DPA addressed a few complaints lodged by individuals against the availability of (past) newspaper articles via a newspaper's online historical archive. The requests pointed out that the archived reports no longer mirrored the current situation, as the individuals had subsequently changed their lives for better. The DPA has found that such availability serves purposes of (historical) research and analysis; accordingly, the data subjects' consent is not required and the data may be processed beyond the time necessary to achieve the initial purposes. The processing is lawful and relevant; the data should not be erased and/or anonymised as requested by the complainants. However, the data retrieval mechanisms of external search engines impact on the complainants' rights disproportionately as they forever link up the given individual to past events and behaviour; additionally, the information in question can be disseminated on the Internet for purposes unrelated to historical research due to the current retention mechanisms of search strings. The complaints were granted in part – i.e. the web pages containing the complainants' personal data should not be indexed by the most popular external search engines using the complainants' names, but they should be left unchanged within the publisher's online archive (accessible via the publisher's website). Technical tools are currently available to meet this requirement ("Robots Exclusion Protocol"; use of the "Robots Meta Tag"). The publisher was ordered to comply within 60 days. The DPA reserved the right to carry out more in-depth inquiries into the broader implications of this issue, with the cooperation of all the relevant stakeholders.

Paternity Tests without Child's Consent for Judicial Purposes: A complaint addressed the case of a father who had performed a genetic test on his son without informing him, in connection with investigations he was carrying out to establish consanguinity. A private investigation agency had collected two cigarette butts binned by the man's son, acting on instructions of the

man's legal counsel. The biological samples had been tested, without informing the data subject, to establish genetic compatibility between father and son. The Italian DPA ruled that a paternity/maternity test may not be performed without the child's consent if such test is not indispensable for judicial purposes. The DPA recalled that genetic data may only be collected and processed with the data subject's "prior, written" and informed consent. This requirement may only be derogated from to establish or defend a judicial claim; however, this only applies if the test is absolutely "indispensable" and is carried out pursuant to the conditions set forth by the Italian DPA – which include, in particular, an obligation to provide specific information to the data subject if the genetic test is aimed at establishing paternity/maternity. The DPA found that the son's data protection rights had been violated and prohibited both his father and the legal counsel from further processing the genetic information that had been unlawfully collected in the manner described above.

Business Information: Several complaints were lodged in the past year against a company managing the largest business information database in Italy, providing banks, financial agencies, professionals, and companies with information on business reliability and performance. As well as handling the many complaints concerning this topic, the Italian DPA tackled the broader issue via a decision that was targeted specifically at the company in question (see above).

Inspections

Inspection activities were enhanced further in 2008, in line with the general upward trend reported for the previous years. The activities focused on issues of general interest for several categories of data subject. More specifically, demanding in-depth inspections were carried out into the processing operations performed by a. financial and taxation bodies; b. banking institutions; c. business information companies; d. telecom operators, in relation to unsolicited marketing; telecom operators, in relation to customer profiling based on traffic data; f. consumer credit organisations; e. companies re-using public data, in particular electoral lists and data contained in public registers of movable and immovable property. Many inspections were performed with respect to public and private entities using video surveillance systems, in order to check that the processing was lawful and compliant with the general decision issued by the Italian DPA in this respect. Importance should also be attached to the checks carried out on private hospitals processing sensitive data, in relation to the adoption of minimum security measures.

Latvia

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

Personal Data Protection Law

Directive 95/46/EC is transposed into national law by the Personal Data Protection Law that came into force on 20 April 2000. The most recent amendments came into force in 6 March 2008. The Personal Data Protection Law was amended on 21 February 2008 and the main changes were related to the exception to a data subject's rights of access to data when data processing is carried out for state interests in taxation matters and regarding data processing of insurance companies with the aim of claiming indemnification in accordance with an insurance contract.

Law on Data State Inspectorate

In order to ensure complete independence of the Data State Inspectorate of Latvia, the process of drawing up the draft Law on Data State Inspectorate was completed. In light of the need to review the means required for the operations of the independent data protection authority in correspondence with the economical situation in Latvia, the draft law was updated at the end of 2008 and beginning of 2009. It is expected to be submitted to the government by mid-2009.

Regulation on data transfer to third countries

In 2008, the Data State Inspectorate of Latvia continued its activities for drawing up the Regulations of the Cabinet of Ministers on Standard requirements for agreements for personal data transfer to third countries. The regulation implements the requirements regarding content of contracts stipulated in the Commission's Decisions 2001/497/EC and 2004/915/EC on Standard Contractual Clauses for the transfer of personal data.

Regulation on training and examination of the data protection officers

The Personal Data Protection Law provides for the notification of data processing. Since 2008, there has been an alternative option – the data protection officer within private and public institutions. The Data State Inspectorate has therefore drawn up the Cabinet of Ministers Regulations (5 February 2008 No.80) "Procedure on the data protection officers' training" that came into force in 9 February 2008. The regulation specifies the procedure of training and examination of data protection officers as well as the training programme. The training can be carried out by the Data State Inspectorate and other public or private sector institutions, but the exam is provided only by the Data State Inspectorate. In 2008, the Data State Inspectorate of Latvia organised two examinations, and certificates were issued to seven data protection officers who represent both the private and governmental sectors.

Higher fines for illegal actions relating to personal data

On 3 July 2008 the Latvian Administrative Violations Code was amended thus establishing higher fines for illegal actions relating to personal data. The amendments came into force on 7 August 2008 and the highest fine to be applied to legal persons is now 10,000 lats (approximately €14,230).

Regulations on data retention of Electronic communication services for law enforcement purposes

Directive 2002/58/EC and Directive 2006/24/EC are transposed into national law by the Electronic Communications Law.

From 2007, the Data State Inspectorate has been the authority responsible 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 communications service providers in accordance with Article 19 of the Electronic Communications 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*. The Regulations of the Cabinet of Ministers (4 December 2007 No.820), the "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 and submit the statistical information on the requested retention data" specify the time frame for how long the electronic communication service providers are obliged to store and submit the statistical data to the Data State Inspectorate. 2008 was the first year in which the Data State Inspectorate of Latvia summarised the statistics.

B. Major case law

The Data State Inspectorate received 140 complaints during 2008, mostly related to personal data processing without any legal basis and data processing to an extent that exceeds the purpose of data processing. As a result of inspections in the field of personal data protection, violations of Personal Data Protection Law have been confirmed in 28 cases. In 18 % of cases warnings were issued, compared to 2007 when warnings were issued in 10 % of cases. The percentage has therefore increased. In addition, the number of administrative fees imposed upon violators in 2008 has increased by approximately 40 % compared to 2007. The complaints mostly related to data processing without legal bases, and violation of data subjects' rights (Article 10 and 11 of Directive 95/46/EC) and violation of the proportionality principle in data processing.

Most common violations of personal data processing were related to:
- publishing the personal data on the Internet;
- video surveillance;
- copying passports;
- data processing carried out by house maintenance services;
- data processing of credit reference agencies and data transfer to third persons.

Compared to 2007, the number of violations in 2008 regarding the publication of personal data on the Internet has increased. In addition, cooperation with the police was increased with respect to cases when persons are using personal data of another person instead of their own personal data during processes in which the identity of suspected persons was clarified.

C. Major specific issues

These are the main issues of 2008 in which the Data State Inspectorate participated in discussions at the national level. The main issues were related to:
- drawing up the concept on the national eHealth system;
- organisation of the vehicle insurance policy online-purchasing system and solving the issue of ensuring the rights of disabled persons to a discount on vehicle insurance as it involves access to sensitive data;
- considerations at national level regarding passenger data transfer to USA and exchange of personal data with USA as part of the Visa Waiver Program;
- setting up the joint database of biometric data and biometric data processing in passports.

Specific cases (related to the main issues for which complaints were received):
1. A significant proportion of received complaints was related to credit reference. Personal data of debtors are transferred to third persons for the purpose of debt recovery. In addition, the current and historical data are transferred to third persons without the consent of the data subject. In most cases transfer of personal data to third persons is considered as data processing without legal basis and exceeds the scope of data processing.
2. The publication of personal data on the Internet without the consent of data subjects can be often violation of Personal Data Protection Act. Such an action by the data controller is considered to be data processing without legal basis.
3. The employer has transferred to third persons copies of ID documents taken from his employees and clients. The copying of ID documents is considered as excessive personal data processing, and transfer of personal data to third persons is considered to be data processing without legal basis and exceeds the scope of data processing.

Drafted recommendations
In 2008, the Data State Inspectorate drafted two recommendations. Taking into account the number of complaints regarding the usage of video surveillance and SPAM, and in order to promote understanding of those issues, the Data State Inspectorate drafted:

- the Recommendation on Data Processing regarding Video Surveillance;
- the Recommendation on Commercial Communications.

Schengen Information System (SIS).
In 2008, the Data State Inspectorate carried out inspections for institutions and authorities who have access to the Schengen Information System (SIS). The control activities were carried out in accordance with Article 96, Article 97 and Article 98 of Schengen Convention.

Data protection in schools
In 2008, the Data State Inspectorate organised several workshops for teachers and other administrative school personnel regarding data protection in schools. The general data protection principles were explained and specific issues were discussed, including access to school results (the "e-class" project), publication of the information in school web pages, storage of medical data, video surveillance, etc.

Lithuania

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

On 1 February 2008 the Seimas of the Republic of Lithuania (the Parliament) adopted an Amendment to the Law on Legal Protection of Personal Data (the new wording will enter into force on 1 January 2009).

The new wording sets out the provisions of the Law on Legal Protection of Personal Data regulating the processing of the personal identification code. Data controllers using automated data processing means for personal health related data for the purpose of health protection and processing personal data for scientific medical research purposes, must notify the State Data Protection Inspectorate and apply for a prior check. The term "video surveillance" has been defined and regulations have been adopted regarding the processing of personal image data, and personal data for direct marketing and solvency evaluation purposes. In addition, regulations have been adopted regarding the status of a person or a unit, responsible for data protection and the complaints handling procedure. The wording of the new Law on Legal Protection of Personal Data establishes the independence of the State Data Protection Inspectorate functioning as a supervisory institution for data protection (as understood in terms of Directive 95/46/EC) and provides for a 5 year term of office for the Head of the Inspectorate.

On 14 November 2008, the Law on Amendment of and Supplement to the Law on Electronic Communications of the Republic of Lithuania (entry into force 15 March 2009) was adopted, transposing the provisions of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The law stipulates that the traffic data of the subscriber or registered user of electronic communications services may be stored for no longer than 6 months from the date of communication, except for cases where the bill is lawfully disputed or the data are necessary for debt recovery, and also in those cases referred to in Article 77(2) of this Law. In order to ensure access to data in cases of serious and very serious crimes, as described in the Penal Code of the Republic of Lithuania, where such information is necessary for the purpose of investigation, detection and prosecution of criminal acts, the providers of public communications networks and/or public electronic communications services must store the information for a period of 6 months from the date of communication and in accordance with the procedure established by the laws, to provide the competent institutions free of charge with the data generated or processed by them. The duty of data storage also includes retention of data related to unsuccessful calls being generated or processed and stored (telephony data) or recorded (Internet data) by the providers of public communications networks and/or public electronic communications services in providing the appropriate services.

If the above-stated data are necessary for the entities of operational activities, the pre-trial investigation institutions, prosecutor, court or judge to prevent, investigate and detect criminal acts, the institutions authorised by the Government - on instruction from the entities of operational activities - the entities providing electronic communications networks and/or services must store such information for a longer period, but no longer than an additional six months. Such storage shall be paid for by state funds in accordance with the procedure established by the Government (Article 77(2) of the Law on Electronic Communications of the Republic of Lithuania).

On 12 November 2008, by Order of the Director of the State Data Protection Inspectorate No 1T-71 (1.12) "On the Approval of General Requirements for the Organisational and Technical Data Protection Measures" General Requirements for Organisational and Technical Data Protection Measures were ratified. They specify the general requirements for organisational and technical data protection measures, which should be implemented by a data controller and data processor to guarantee personal data against any accidental or unlawful destruction, alteration, disclosure and against any other unlawful processing.

B. Major case law

Publication of the personal data of drunken persons on Internet

The State Data Protection Inspectorate received 2 complaints concerning publication of personal data on the website of Vilnius City Police Headquarters. After the investigation the State Data Protection Inspectorate found that the Head of Vilnius City Police Headquarters made the decision to publish personal data (first name, surname, year of birth, time and place of the committed administrative offence, degree of drunkenness, and the sanction imposed) of the persons who committed administrative offences of drunken driving on the website of Vilnius City Police Headquarters. The purposes of such personal data publication were informing the public, education and prevention of administrative offences.

The State Data Protection Inspectorate decided that such actions by the Police were illegal since the purpose of collecting the personal data of the complainants was to impose a penalty. Later, the personal data of the complainants were processed in the Register of Road Traffic Rules Offences and Traffic Accidents. According to the paragraph 2 of the Article 6 of the Law on Police Activities, it is prohibited to disclose personal information which is stored in the police information systems to other persons, unless otherwise provided for by laws and other legal acts. According to the subparagraph 1, paragraph 1, Article 3 of the Law on Legal Protection of Personal Data, the data controller must ensure that personal data are collected for specified and legitimate purposes and are not subsequently processed for purposes incompatible with the established purposes before the personal data concerned are collected. In the opinion of the State Data Protection Inspectorate such personal data could not be published on the Internet for the purposes of informing the public, education and prevention of administrative offences because:

- these purposes are different from the purposes determined before the collection of personal data;
- according to the Law on Police Activities it is prohibited to disclose the personal information which is stored in the register;
- there were no criteria for lawful processing of personal data.

The State Data Protection Inspectorate issued an instruction to the Vilnius City Police Headquarters demanding the cessation of publication of personal data related to persons fined for offending Road traffic rules (their name, full name, year of birth, the time and location of the administrative law violation committed by them, the established degree of drunkenness, the article of the Code of Administrative Offences of the Republic of Lithuania envisaging liability for the committed administrative offence and the sanction imposed for the violation) on the web page produced for the purpose of informing the public, education and prevention of violations of administrative law.

Vilnius City Police Headquarters appealed against the decisions of the State Data Protection Inspectorate in court. Vilnius District Administrative Court concluded that subparagraph 6, paragraph 1, Article 5 of the Law on Legal Protection of Personal Data should be applied (personal data may be processed if processing is necessary for the purpose of legitimate interests pursued by the data controller or by a third party to whom the personal data are disclosed, unless such interests are overridden by the interests of the data subject). In addition, this court stated that data such as time and place of the committed administrative offence, degree of drunkenness, imposed sanctions could not even be considered as personal data.

An appeal was lodged against the decision of Vilnius District Administrative Court with the Supreme Administrative Court of Lithuania.

The Supreme Administrative Court of Lithuania concluded that data such as time and place of the committed administrative offence, degree of drunkenness and imposed sanctions should be considered as personal data when these data are published together with the first name and the surname of the data subject.

The Court also ruled that the Vilnius City Police Headquarters have been disclosing personal data on its website under the guise of legitimate interest (subparagraph 6, paragraph 1, Article 5 of the Law on Legal Protection of Personal Data). Summarising the provisions set out in the Code of Administrative Offences, it shall be concluded, that

the Code of Administrative Offences obliges state institutions, including the Police, not only to explain the committed offences and impose an appropriate sanction but also to develop and implement measures preventing administrative offences. In addition, the Code of Administrative Offences stipulates that the prevention of offences is one of the purposes for imposing the administrative penalties. Thus, it becomes apparent that the preventive measures related to the imposed administrative penalties may be drafted and implemented on the basis of information, including personal data, collected in the course of the proceedings of administrative offences.

According to judicial practice, drunken driving of motor vehicles is qualified as a very serious offence against Road Traffic Rules. The Code of Administrative Offences provides the strictest sanctions for such offences, because these offences directly endanger the health and safety of road users. Therefore, comparing the balance between the values: on the one hand, the temporary publication (one month) of personal data of an individual who has committed a serious administrative offence, and, on the other hand, the prevention of a threat to lives, health and safety of road users, the court came to the conclusion that, in this case, the data subject's right to privacy is less important than the public interest to perform prevention of serious offences of Road Traffic Rules. The interests of the data subject do not override the legitimate interest of the Police.

Personal data publication on the Internet for electoral purposes

The Central Electoral Commission of the Republic of Lithuania notified the State Data Protection Inspectorate about processing of personal data of parliamentary candidates' on the Internet so that the State Data Protection Inspectorate can perform a prior check and issue a permit for such processing. According to the rules submitted by the Central Electoral Commission of the Republic of Lithuania, personal data (first name, surname, the political party, date and place of birth, citizenship, nationality, family status, names of family members, declarations of property and private interests, etc.) of the candidates are available on the website of the Central Electoral Commission of the Republic of Lithuania for an unlimited time. The unlimited time for publication of personal data does not depend on whether or not the candidate won the elections and became a Member of Parliament.

According to Article 4 of the Law on Legal Protection of Personal Data, personal data shall not be stored longer than necessary for data processing purposes. When personal data are no longer needed for processing purposes, they must be destroyed. Following this provision, the State Data Protection Inspectorate issued an instruction to the Central Electoral Commission of the Republic of Lithuania to determine how long the personal data of the candidates should be published on the Internet. The Central Electoral Commission of the Republic of Lithuania denied setting a limited period and the State Data Protection Inspectorate decided to refuse an authorisation to the Central Electoral Commission of the Republic of Lithuania to publish personal data of the candidates on their website.

The Central Electoral Commission of the Republic of Lithuania appealed against the decision of the State Data Protection Inspectorate.

Vilnius District Administrative Court decided that the decision of the State Data Protection Inspectorate is legitimate and there are no reasons why the Central Electoral Commission of the Republic of Lithuania should be authorised to publish such personal data on its website for an unlimited time.

An appeal was lodged against the decision of Vilnius District Administrative Court with the Supreme Administrative Court of Lithuania.

Different decision laid down by the Supreme Administrative Court of Lithuania.

The Central Electoral Commission of the Republic of Lithuania processes personal data in order to inform the electors so that they can exercise their effective electoral right. There is no doubt that the data concerning the Member of Parliament candidates are necessary during electoral campaigning. Information regarding those who ran for Parliament and those who have won the term

of office as Member of Parliament, as well as persons who were not elected, is still indisputably relevant to the process of calculating and announcing the election results. Once the Member of Parliament has taken an oath, the elector has a reasonable cause to know who is representing his interests. Likewise, during the term of office of the elected Member of Parliament, in principle, it is still possible to fill a vacancy for the candidate who did not get into Parliament. In light of this, the data related to Member of Parliament candidates and the winners of the seats in the Parliament is of great concern to the electors and remains topical from the time of self-determination to run for the Parliament seat till the end of the term of office.

The unlimited time for publication of the candidates' documents on candidates might be justified by the importance of elections being a form of state governing by involvement of citizens. The democratic elections are an important form of the state governing by participation of citizens, and therefore also an essential asset in forming the state's political representative institutions. The elections shall not be considered democratic and the results – legitimate and legal if they are organised without complying with the principles of democratic elections established by Constitution, in violation of democratic electoral procedures.

Ensuring that the electors are properly informed is a prerequisite to ensuring legitimate and legal elections. Furthermore, the more data there is, the more the confidence of electors is stimulated not only in specific candidates but also in the representative authorities themselves: the electors may access data concerning former elections and how they were organised, find information about former candidacies, collate data and make their choice as to not only the acceptable candidates, but also verify whether the organisation of election procedures is trustworthy, and decide whether they want to participate in elections in general. Therefore the formation of the specific archives on elections and data disclosure may be justified by the legitimate purpose to be achieved – to promote the electors' confidence in the representative institutions themselves.

Having considered that the disclosure of information with reference to the Members of Parliament is in compliance with the legitimate purposes – to promote the electors' confidence in the procedure for the formation of representative institutions, to ensure that the election procedures are legal and transparent, and that the achievement of such aims is significant not only during the specific elections, the Supreme Administrative Court of Lithuania stated that the data regarding elections may be disclosed for an unlimited time.

C. Major specific issues

Personal data processing in financial institutions

State Data Protection Inspectorate with the aim of discovering the scope and the lawfulness of personal data processing of individuals referring to the financial institutions for the speedy credit services by Internet or SMS, performed inspections on the lawful processing of personal data at six financial institutions. The inspections revealed the methods of personal (the clients) identification: a person produces a document confirming personal identity; a person registers and pays from his personal bank account, where the data coincide, a person receives an SMS message with a log-in password; a person fills in a request on the Internet or by phone and after that he inevitably visits customer service in person in order to sign a contract, bringing with him the personal identification document; a person registers by SMS message or Internet and pays from the personal bank account, indicated during registration, and if the data match, he receives an SMS message with the log-in password; a person enters his phone number on the Internet and receives an SMS message with a code which must be entered on the website, and fills in the request form, and pays a fixed fee from his personal bank account. One financial institution established a requirement that copies of personal documents of people who are not users of the electronic banking service, should be sent to it by fax or e-mail for personal identification. In the opinion of State Data Protection Inspectorate such remote provision of a personal identity document may not be considered a proper means for personal identification.

The data provided by persons are verified by referring to different data controllers: one company receives the data about the proceeds persons receive from

the State Social Insurance Fund Board under the Ministry of Social Security and Labour of the Republic of Lithuania; three financial institutions receive data from Residents' Register Service under the Ministry of the Interior of the Republic of Lithuania for the purpose of personal identification, data revision and checking accuracy; data connected with personal debts are received by all financial institutions from JV "Creditinfo Lietuva" Three financial institutions receive data on real property owned by a person on the Register of Real Property where one of them receives and processes this personal data from Register of Real Property illegally; four financial institutions receive data for the purposes of personal identification and verification from credit institutions (banks).

Various violations of the Law on Legal Protection of Personal Data of the Republic of Lithuania were revealed during the course of the inspection (regarding the amount of personal data; on unlawful data processing without the obtained data subject's consent; on direct marketing regulation and performance (without allowing the data subject to express his consent, to process personal data for the purpose of direct marketing or having established only the right to refuse); on implementation of proper organisational and technical measures). The State Data Protection Inspectorate issued instructions to the investigated financial institutions.

Public awareness

On 23 January 2008, the State Data Protection Inspectorate in conjunction with the Human Rights Committee of the Seimas (Parliament) of the Republic of Lithuania held a conference "European data protection day for youths".

The event marked the European Data Protection Day, which has been traditionally celebrated on 28 January. The aim of the event this year was to draw the attention of the young people of Lithuania and introduce them to the issues of the field that is of the utmost importance to all people, that is, human rights and protection of privacy. The report on the newest identity documents delivered by the representative of Personalisation of Identity Documents Centre under the Ministry of the Interior of the Republic of Lithuania fostered a lot of curiosity and interest among young people. By organising this event, it was decided that it was very important to ascertain how aware young people - teenagers - were of issues on human rights and data protection, and to find out what current issues are upsetting them most.

The event gathered as many as 80 schoolchildren from 14 to 18 years of age from Vilnius schools and colleges. The leaflets were distributed to them containing concise information on how to use the Internet safely and also other handout information material.

Luxembourg

A. Implementation of Directive 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)
No amendments to the above-mentioned law were made during the period of 2008.

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)
No amendments to the above-mentioned law were made during the period of 2008.

Decrees and secondary legislation
The grand-ducal regulation of 7 October 2008 endorses the renewal of the mandates for each of the three effective members of the CNPD, as well as the appointment of two new substitute members.

The government also enacted a grand-ducal Regulation dated 1 December 2008 setting forth the technical specifications for the interception of electronic communications in Luxembourg.

Other legislative developments
The bill determining the "*conditions in which magistrates and police officers may have access to certain databases held by public legal persons*" was adopted by Parliament and published in the Official Gazette of 27 August 2008. The first draft of this text had been commented upon by the CNPD during 2006. Such advice has been followed by the government by the insertion of a vast number of safeguards and security measures into the text, as suggested by the Commission Nationale. During the debates in Parliament, the additional concerns expressed by the Advisory Commission on Human Rights have led to additional restrictive and protective provisions. The adopted law contains a vast panoply of restrictions and valuable guarantees against any possible abuse of such personal data. However it appears that the provisions seem to be too restrictive for the police force to be able to accomplish its day-to-day tasks. Therefore, it might be possible that Parliament will be seized again during 2009 in order to amend these restrictive provisions.

The Commission Nationale advised the government on a vast array of draft bills and grand-ducal regulations, e.g. the draft grand-ducal regulation regarding the collection and processing of personal data of pupils, and the grand-ducal regulation concerning the conditions and modalities for the deliverance of cadastral documentation or the bill amending the electoral law of 2003. Other topics included the draft bill on the free circulation of people and immigration as well as its draft grand-ducal regulation. The latter specifically sets out the categories of personal data to which the Minister having Immigration within its attributions may have access in order to carry out all the necessary controls enacted by the law. Furthermore, the CNPD advised the government on the bill relating to the exercise of the profession of doctor, dentist and veterinarian as well as the draft grand-ducal regulation relating thereto.

The Commission Nationale has also issued advice to the government relating to the recording of emergency numbers in accordance with the law concerning the processing of personal data and the protection of privacy in the electronic communications sector.

B. Major case law

Civil and criminal case law
District Court of Luxembourg, Court of Appeals, 5th correctional chamber on the validity of proof (video-surveillance images) collected in violation of the law of 2002 on data protection

In 2007, the Supreme Court of Appeals ("*Cour de Cassation*") rescinded a decision of the Court of Appeals regarding the validity of proof collected in violation of data protection provisions. The Supreme Court of Appeals based its decision on a breach of the right to a fair trial (Article 6 of the European Convention on Human Rights).

On 26 February 2008, the Court of Appeals (otherwise composed) ruled 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, 16th correctional chamber on the breach of Articles 10, 11 and 14 of the law of 2002 on data protection

On 27 October 2008, the District Court of Luxembourg, 16th correctional chamber added new case law with respect to criminal convictions of an individual on the basis of the law of 2002. An employee working at a cemetery had installed a system of video-cameras inside said cemetery, in its immediate vicinity as well as in the morgue. However, he did not have prior authorisation for the processing of personal data from the *Commission Nationale pour la Protection des Données*, as required by the provisions of the modified law of 2002. As the employee nevertheless proceeded to process personal data (i.e. real-time surveillance of people, saving image data files on his computer and reproducing some scenes for his "*own amusement*"), the court held that he had clearly infringed the provisions of the law of 2002 on data protection and was consequently held liable for these actions.

C. Major specific issues

Cyber-surveillance of employees by the employer
The CNPD has drafted a fundamental decision in the domain of employee cyber-surveillance aiming to strike a balance between respecting a data subjects' private life at work and an employer's legitimate interests.

The principles set out in said decision are taking into account the sheer number of authorisation and information requests received by the CNPD in relation to this matter. The decision advocates a moderate usage of surveillance tools and defines the allowable range of the surveillance measures which may be taken by an employer. Thus, such surveillance may only be carried out for certain purposes, such as safeguarding the functionality of the IT system, the company's industrial secrets and confidential information, as well as preventing unfair competition.

A major difficulty for cyber-surveillance in this domain consists of distinguishing between private life and professional usage. The CNPD maintained that files and messages saved on the employee's workstation are to be considered as professional, unless marked as private.

Private messages may not be opened or read by the employer, even if the use of mailing systems for private purposes has been prohibited beforehand. Moreover, the employer may only open or read files marked as private in the employee's presence.

Professional files and messages may however be accessed while the employee is absent or after his or her departure, in order to guarantee the continuity of the company's workflow (but not to evaluate the employee or take legal action against him or her).

In order to keep a balance between the different parties' legitimate interests, total or permanent supervision is prohibited. Cyber-surveillance must therefore be of a limited scope and may only be increased on the basis of justified and tangible evidence of abuse.

E-Catering - automatic capture of children's canteen attendance
At the CNPD's request, the State Department for Education has reduced the data categories collected as well as the storage period of such data. The right of data subjects to object to their data being collected and processed is also guaranteed. This action is part of a European effort to reinforce children's right to a private life, particularly in a school environment.

Audit of the main Luxembourg telecommunication companies
During the 2007-2008 period, the CNPD carried out an exhaustive audit of the main Luxembourg telecommunication companies. The aim pursued by the CNPD was to obtain an overview of how the telecommunication operators brought their business

into compliance with the provisions of the law of 30 May 2005, implementing Directive 2002/58/EC.

Information and awareness raising campaign
During 2008, the Commission Nationale pursued its information and awareness raising campaign, among others, by actively participating in the works of the National Ethics Committee for Research as well as in the second 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 Luxembourg media.

Malta

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

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 force in July 2003, establishing a transitional period for notification of automated processing operations by July 2004. The provisions in relation to manual filing systems have come into effect in October 2007.

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

Other legislative developments

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, and amending Directive 2002/58/EC, was transposed in the local statute by means of two legal instruments which amended the aforesaid regulations. LN 198 of 2008, amending LN 16 of 2003, and LN 199 of 2008, amending LN 19 of 2003, have been both published in the Government Gazette and came into effect on 29 August 2008.

The regulations oblige service providers to retain the information established under the Directive, for a period of one year in case of telephony and mobile data and for a period of six months in case of Internet related data. Such information can be disclosed solely to the Police or the Security Service, upon their request, and only in cases of serious crimes.

B. Major case law

None to report.

C. Major specific issues

During the year under review the Office held regular meetings with representatives from the various sectors with the main objective to discuss data protection issues applicable to the sector. The continuous drive to communicate with the sectors delivers a high degree of positive feedback which the Office requires for the development of guidelines and codes of practice which will ultimately regulate all the sectors. In this respect, meetings were held with various constituted bodies and also entities from the education, social work, telecommunications, tourism, media, financial services and the health sectors respectively. Discussions were also held with various authorities, including the Malta Communications Authority, the Malta Financial Services Authority, the Malta Resources Authority and the Malta Transport Authority. The Commissioner held also meetings with the Ombudsman, high-ranking officials from the Malta Police Force and officials from the Malta Security Services.

During 2008, the Office received 31 complaints which prompted the Commissioner to investigate each case and communicate his decision according to the outcome of the investigations and considerations factored in the process. The most common subjects of the complaints related to the installation of CCTVs by private individuals, the sending of electronic communications for the purposes of direct marketing without satisfying the criteria established by law and the introduction of biometric systems at the workplace without submitting a prior notification to the Office.

During the period under review, the Commissioner carried out numerous inspections on the processing of personal data undertaken by various data controllers; these inspections were carried out in the course of investigating complaints, as part of the Office's strategy to evaluate a particular sector, on the Commissioner's own motion and also to honour European obligations.

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.

In line with the Office's strategy to raise data protection awareness, presentations were delivered to various organisations and constituted bodies with the objective to 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 on the radio and television programmes. Citizens are becoming aware of their rights and this can be quantified by the substantial number of queries, both by telephone and by e-mail, which have reached the Office during such period.

On 28 January, the Data Protection Commissioner joined the other Data Protection authorities in Europe to celebrate the Data Protection Day. To mark the Day, this Office distributed posters and mouse mats in schools with the objective to raise awareness amongst the younger generation. This is in line with the Office's firm commitment to inculcate the new privacy culture in children to enable them to appreciate and exercise such fundamental rights. This year's message related to the use of Internet and the importance to be aware of the potential privacy risks that the individual's personal data might be exposed to when provided on the Internet.The Office stressed that the data subject's identity is valuable and therefore it is imperative to keep it safe. As part of the activities, with the assistance of the Office of the Prime Minister, the Commissioner also addressed all the Data Protection Officers within the Public Service.

In June, a Bill entitled 'Freedom of Information Act' was presented in Parliament. It establishes the right to information held by public authorities in order to promote added transparency and accountability in government. The Bill will vest the Data Protection Commissioner with the additional functions and duties of Information Commissioner when the Bill is brought into force.

During this year, the Office suffered the loss of the Data Protection Commissioner, Mr Paul Mifsud-Cremona, who passed away on 14 August. Mr Mifsud-Cremona had occupied this position since 1 January 2004. In December, the Prime Minister, following consultation and in agreement with the leader of the Opposition, nominated Mr Joseph Ebejer as the new Data Protection Commissioner. The new Commissioner is expected to be formally appointed early next year.

Netherlands

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

Directive 95/46/EC was transposed into national law, the Wet bescherming persoonsgegevens (Wbp - Dutch Data Protection Act). This was done by Act of 6 July 2000[19] and came 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 came into force on 19 May 2004[20]. Other legislation transposing parts of this directive are, amongst others, the *Wet op de Economische Delicten* (Act on Economic Offences), implementing article 13(4) of Directive 2002/58/EC.

B. Major case law and major specific issues

Last year, the Dutch Data Protection Authority (Dutch DPA - College bescherming persoonsgegevens, CBP) was able to strongly improve its positioning as supervisory body. Its chosen focus is the investigation of compliance with the rules concerning the processing of personal data and enforcement action where legislation is violated. In 2008, the CBP started to systematically do what we said we would do the year before: above all else, deploy our manpower and resources to conduct investigations into how the relevant statutory provisions are being fulfilled and, where the violation of these provisions is observed, take enforcement action. In 2008, the Dutch DPA also makes clearer choices, on the basis of risk analyses, on how to deal with the large number of very different subjects that it is confronted with. The Dutch DPA prioritises structural issues and violations that affect many people - vulnerable groups in particular. The risk analysis was prepared on the basis of a system developed by us and tested by experts and on the basis of warnings that reach us in various ways, with the object of determining the sectors in which (1) many citizens are at a (2) great risk of (3) encountering serious and structural violations of the Wbp. The Dutch DPA 2008 policy plan gained concrete form and content on this basis.

The figures for 2008 are promising: the Dutch DPA carried out supervisory investigations in 95 cases (50 % more than in 2007) and imposed a sanction or threatened to do so in 68 cases, which represents almost double the figure for 2007 (2007: 39; 2006: 2!).

The Internet

Last year, the Dutch DPA received a large number of complaints and warnings about the publication of personal data on the Internet. These relate particularly to requests for the removal of this data and to the rights that an individual has if his or her data is published on the Internet. By taking enforcement action against websites that structurally violate the *Wet bescherming persoonsgegevens* (Wbp) (Dutch Data Protection Act), the Dutch DPA wants to increase the alertness of both controllers and data subjects. Both parties must be more aware of the rights of data subjects and of the need for these rights to be respected.

Emergency action against a website containing the personal data of civil servants and politicians yielded success in record time: access to the site was blocked within just one day. Action against a municipality that published applications for planning permission complete with personal data and the signature of the applicant and the name and signature of the relevant official on its site led to the development of a new online application form that will be used throughout the Netherlands. As a result, the unlawful publication of this personal data has been stopped.

The covert registration of the IP addresses of visitors to the website Geencommentaar.nl (nocomment), with the object of making this list accessible to others, was declared unlawful by the Dutch DPA. In response, the controller stated that the list had been destroyed and the software removed from the site. The website beoordeelmijnleraar.nl (assessmyteacher) was also declared unlawful. The website holder

[19] 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

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

subsequently made a number of changes to the site. Together with the Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA) (Independent Post and Telecommunications Authority), the Dutch DPA was successful in its efforts to deal with services that facilitate reverse searches – using a telephone number to find the corresponding name and address details – and in the specification of the conditions under which viral marketing is permitted.

Business and work
Medical data on employees is of a very sensitive nature. Further to the investigation of an occupational health and safety service, the Dutch DPA suspects that other occupational health and safety services also systematically disclose these data to employers. Because of this, the decision was made to examine data processing by other occupational health and safety services as well. The investigation will continue in 2009.

The greatest possible care must also be exercised where data relates to sensitive information about an individual's financial position. The Landelijk Informatiesysteem Schulden (National Debt Information System) submitted a design for a registration system to the Dutch DPA for assessment on two occasions. The design was rejected by the Dutch DPA in both instances. Data processing had been insufficiently demarcated and the group of people with access to these data would have been too large, which would entail the risk of damages to individuals who had been entered into the system erroneously.

One of the structural problems of privacy protection is that many people do not know where their data ends up and what happens to it. If persons are investigated, whether by a private detective agency or the Afdeling Sociale Recherche (Social Security Fraud Department), these persons must be notified thereof when the investigation has been completed. Following its investigation, the Dutch DPA has established that this duty to disclose is still not observed in many cases. The Dutch DPA will continue its vigilance in this respect. Obtaining data that can lead to more efficient and conscious energy use must also take place in line with the Wbp. A number of privacy safeguards were added to the legislative proposal relating to the introduction of smart energy meters following criticism from the Dutch DPA.

Transport
After much wrangling, lasting several years, concerning the use of travel data for marketing purposes following the introduction of the *OV-chipkaart* (public transport chip card) and the publication of a study by the Dutch DPA on the use of the card on the Amsterdam metro network, the public transport companies eventually came up with a system that satisfies the requirements of the Wbp. The Dutch DPA will monitor the implementation and compliance with the standards laid down. An official investigation in 2008 into the processing of personal data for the purpose of the chip card, which will be compulsory for the Rotterdam metro with effect from 29 January 2009, led to the conclusion that there is no reason to take any further steps at this stage. The kilometre price system may also lead to a detailed image of travel behaviour, in this case concerning individual motorists. The Dutch DPA has advocated data minimisation in the Lower House.

The monitoring of cars that use certain routes involves all citizens who drive cars, including those who have nothing to hide. The Dutch DPA has developed guidelines for Automatic Number Plate Recognition (ANPR), which are intended to bring an end to the lack of clarity on what is and what is not allowed in the implementation of this method. The police are not allowed to retain and process any scanned data. A situation must be avoided where all motorists are regarded as potential suspects.

Healthcare
Extra care and proper security are required when processing data on someone's health. In the legislative proposal that provides for the Electronic Patient File, consideration is given to the highly critical advice issued by the Dutch DPA in this respect. In principle, only professionals with a treatment relationship with patients will have access to their medical records.

The Dutch DPA points to the need for citizens, and patients in particular, to have the right to know who has access to their data, when and how, and the right to know that this data is processed securely in other healthcare areas in which personal data is exchanged as well. This applies when health insurance companies provide data to the central administration office on insured parties with health problems who are eligible for an allowance.

It applies when one insurer discloses personal data to another insurer when collective contracts are transferred. It applies for the national processing of data for care registration across the board under the Algemene wet bijzondere ziektekosten (Exceptional Medical Expenses Act). It applies when issuing personal data to the College voor Zorgverzekeringen (Care Insurance Board) for the purpose of the collection of premiums for health insurance from defaulters. It also applies to the use of the Burgerservicenummer (BSN) (Citizens Service Number (CSN)) in the healthcare sector: the processing and provision of personal data must comply with a certain level of information security.

Compliance with the level of information security required should not always be assumed, as became clear from an investigation that the Dutch DPA conducted with the Inspectie voor de Gezondheidszorg (Healthcare Inspectorate). None of the 20 hospitals investigated complied with this standard, which may have serious consequences for the quality of care provided and for patient privacy. The hospitals must demonstrate that they will comply with the standard and how they will do this.

Young persons

The digital processing of personal data in general and by the government in particular explicitly demands safeguards. This applies all the more where information relates to children and young persons.

In 2008, the Dutch DPA issued highly critical advice on the draft legislative proposal that would result in the creation of a Verwijsindex Risicojongeren (reference index for young persons at risk). In the opinion of the Dutch DPA, the proposal is contrary to the Wbp. Criticism focuses particularly on the object of the reference index, which is not specific enough, combined with its unclear criteria for the registration of a young person by his or her care provider, entails an almost inevitable risk of arbitrariness. Although the legislative proposal submitted on 6 February 2009 responds to the criticism raised by the Dutch DPA – amongst others – in several areas, the essence unfortunately remains the same.

It is often claimed that privacy regulations prevent the proper implementation of child protection measures. This myth was dispelled during a round table conference in April 2007, between the Dutch DPA and professionals in the field of youth care. The Dutch DPA is able to agree to the draft legislative proposal on the amendment of the child protection measures that introduces a *right* to speak. If the interests of the child make it necessary to break (doctor-patient) confidentiality, the care provider must be able to exercise his right to speak.

Primary schools issue educational reports on their pupils to secondary schools. The Dutch DPA has investigated compliance with the information obligation to the parents of children in this situation. This is vital for the possibility of correcting the report, which can have a protracted negative effect on children if it contains incorrect or outdated information.

Police and the judicial authorities

The serious misuse of personal data in the form of identity fraud is also set to increase in the Netherlands. To combat this theft of someone's personal data, compliance with the information obligation is vital, so that the data subject knows that an organisation is processing his or her personal data and which data is concerned. In 2008, via meetings with experts and a study of literature, the Dutch DPA explored the different ways in which identity fraud could be prevented and combated.

Safeguarding the correct and transparent use of personal data is also vital in light of the increased powers that police and the judicial authorities have in relation to the processing of personal data. In 2007, the Dutch DPA took the view that legislation that opens up the possibility for a DNA family relationship investigation as part of criminal proceedings is in violation of the Wbp. The Minister took the criticism raised by the Dutch DPA into consideration in a second proposal in October 2008.

As regards the proposal by the Openbaar Ministerie (Public Prosecution Department) to extend investigation reports – through the use of the Internet and telephone, for instance – the Dutch DPA advised on the inclusion of appropriate safeguards in order to ensure that these reports are protected from search engines and that any mistakes are rectified quickly. The *Aanwijzing opsporingsberichtgeving* (Instructions on investigation reports) will be modified further to this criticism. The

Dutch DPA also issued critical advice on the provision of criminal data from the Public Prosecution databases to data subjects and third parties for purposes not relating to the criminal procedure. The Dutch DPA feels that this is only allowed in certain cases and only where absolutely necessary. Advisability alone is not enough.

The Dutch DPA issued an investigation report on the internal exchange of personal data within the police forces via the police information desk. By far the majority of police regions were found to be completely unequipped for compliance with the requirements of the Wet politiegegevens (Police Data Act), which became effective on 1 January 2008.

Poland

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

During the reporting period, the Inspector General for Personal Data Protection took actions in order to introduce amendments to the Data Protection Act concerning *inter alia*: improved efficiency of the enforcement of administrative decisions issued by data protection authority with regard to non-financial obligations; introduction of a penal provision in the case of prevention or hampering of inspection activities, into the Data Protection Act; specification of the provisions of the Data Protection Act concerning the contents of inspection protocol; regulation of the withdrawal of consent for the processing of personal data (Article 7 (5) of the Act); possibility to establish local units (branches) of the Bureau of the Inspector General for Personal Data Protection; so called approaches to public authorities, self-government units and natural and legal persons who process personal data (introduction of obligation to respond to such approach within 30 days from the date of delivery thereof); repealing of Article 29 of the Data Protection Act (concerning the possibility to disclose personal data for the purposes of inclusion of data into a data filing system or other purposes) – disclosure of personal data is intended to take place solely under the provisions of Article 23 or 27 of the Data Protection Act.

On the Inspector General's initiative a Regulation was passed by the Minister of Internal Affairs and Administration as regards specimen application form for notification of data filing system to registration with the Inspector General. The purpose of introducing the new provisions is to help applicants fill in notification forms at the time of notification of data filing systems to registration as the previous practice revealed that it sometimes caused serious problems to them (most of the fields were replaced with option buttons) and to ensure increased transparency of the form and enshrine the essential obligations of the controllers. It is worth mentioning that the Inspector General had previously issued many decisions of refusal to register a data filing system in the case where mistakes were found in the notification forms, and it therefore had adverse effects for economic activity being carried out by the applicant or even made it impossible to continue with such activity.

B. Major case law

During the reporting period, the legal proceedings concerning a commercial disclosure by Telekomunikacja Polska S.A. (telecom operator) of subscribers' personal data who consented to disclose their personal data ('opt-out') in a telephone directory to third parties were closed. The Administrative Court stated that according to the Inspector General's standpoint, the consent in question (i.e. absence of objection) to the disclosure of data in telephone directory is not an independent prerequisite of disclosure of such data to third parties. In other cases concerning the collection of fees for providing information to data subjects by BIK S.A. (credit information agency) the court supported the Inspector General's view according to which such collection is illegal. The case was submitted before the Supreme Administrative Court and is now awaiting settlement.

Another important decision concerned a prohibition of the processing of personal data recorded in backups from the moment of deletion of such data from the data filing system. The court stated that such practice is not permissible. It was mentioned that an entity which decides to delete data should delete them entirely.

In addition, the Administrative Court issued a decision on the legality of the processing of personal data of bank clients by BIK S.A. for statistical purposes for a period of 12 years (according to paragraph 5, Article 105 of Banking Law). The Inspector General for Personal Data Protection examined, from the point of view of the obligation to disclose public information, the issue of personal data protection included in statements on the financial position of persons who perform functions in public administration authorities. The Inspector General considered that disclosing of residential addresses of persons submitting statements on their financial position and addresses of properties belonging to those persons is illegal. The Inspector General also analysed the issue of disclosure, on the Public Information Bulletin website, of resolutions by the commune council including first names, surnames or residential addresses

of persons those resolutions related to. It was found that disclosure of data that enable a full identification of the persons in question were unnecessary to fulfil the obligation to provide information under the Access to Public Information Act. It was maintained that such practice invades the right to privacy of those persons and the scope of data being disclosed is not relevant to the purpose of disclosure of resolutions. The above-mentioned standpoint was supported by the decision of the Administrative Court.

In 2008, the Inspector General also examined the legitimacy of applications submitted to newspapers' publishers that included a request for disclosure of journalists' personal data which were necessary to bring civil action to the court against those persons in connection with the infringement of personal rights in press publications. In most cases the Inspector General ordered the disclosure of such data, unless requested data were actually necessary to bring civil action against data subjects, and therefore the disclosure was in compliance with the provision of paragraph 2, Article 29 of the Data Protection Act.

C. Major specific issues

In connection with Poland's accession to the Schengen area, it was necessary to examine the accuracy of personal data processing in the Schengen Information System. The entities authorised to have direct access to the National Information System in order to make entries to SIS and access to data included in SIS (Police, Border Guard, customs chambers and consulates) were subject to inspections. In the course of the inspection activities, some irregularities were found (e.g. lack of register of persons authorised to access data included in SIS, lack of written authorisations, no specification of the scope of authorisation to personal data processing and lack of badges for authorised personnel). In this respect, the Inspector General addressed a written request to the Commander in Chief of the Police, Chief of the Border Guard, and Head of Customs Service to take action to eliminate the indicated failings.

In addition, some modifications were made to software used to fill in notification forms at the time of notification of data filing systems to registration in order to minimise the number of errors made by applicants during the preparation of such registration applications and to enable those who do not possess a secure electronic signature to send an application. The modifications made will significantly improve the process of data filing systems registration and facilitate fulfilment of the obligation to notify data filing systems to registration for those who are obliged to do so. The software in question together with the online register of data filing systems combine to form the 'Electronic platform of communication with the Inspector General for Personal Data Protection' (e-GIODO platform).

The analysis on appropriate interpretation of the notion of IP address, electronic mail, cookie files, IMEI number, user name and login was prepared by the Bureau of the Inspector General in response to the increasing number of issues concerning the processing of personal data with the use of modern technologies. The analysis is intended to be a helpful tool for making a legal assessment on whether the above-mentioned information may be regarded as personal data on a case-by-case basis. Moreover, a special modern technology task force was established within the Bureau in order to develop authority standpoints, legal opinions, guidelines, remarks, policies, etc. concerning issues related to the processing of personal data with the use of Information and Communication Technologies in the broad meaning of the term.

Moreover, the Inspector General hosted the 10th Meeting of Central and Eastern European Data Protection Authorities that was held 1-4 June 2008. The issues relating to children's online privacy protection; tasks preformed by Central and Eastern data protection authorities in the context of expanding the Schengen area; qualifications, tasks and powers of data protection officers were *inter alia* discussed, the CEEDPA forum also evaluated the last ten years of its activity. Two final declarations were adopted concerning further cooperation within the forum and concerning equal treatment of the national languages of all EU Member States.

As regards educational activities, the employees of the Bureau of the Inspector General conducted 62 training courses on personal data protection *inter*

alia in: ministries, courts, the Tax Control Office, the National Council of Legal Advisers, the Consulate of the Republic of Poland in Brussels, the National Chamber of Tax Advisers, and the Public Procurement Office (in total we trained about 1 700 people). In relation to Poland's accession to the Schengen area, special training courses on the processing of personal data in SIS for training staff in Police Headquarters and Border Guard were conducted.

Moreover, the new e-learning platform 'eduGIODO' was launched in order to disseminate knowledge on personal data protection in a convenient and modern manner. It provides all interested parties with a wide range of information concerning data protection which is divided into special modules devoted to particular issues (so called 'ABCs'). This 'virtual university' offers different training courses focused on the specific aspect of data protection (data subject rights; general data protection principles and the obligations of the controllers). For the launch of the 'eduGIODO' platform, two nationwide conferences were held (in Warsaw and Gdańsk) where the main objectives of the platform in relation to personal data protection issues were presented.

A workshop on amendments stipulated in EU data protection legislation in the context of the implementation of *acquis communautaire* in the field of personal data protection was organised by the Inspector General for Personal Data Protection within the framework of TAIEX program. The workshop was mainly aimed at judges and prosecutors.

Last year, the employees of the Bureau of the Inspector General for Personal Data Protection participated in the project for exchange of experience of data protection authorities' personnel. The project was implemented within the framework of the Leonardo da Vinci Lifelong learning programme entitled 'New competencies of persons responsible for the enforcement of data protection provisions'. As a result the project contributed to the improvement of knowledge and skills in the field of implementation of community law, exchange of experience concerning operation of data protection authorities, importing practices applied in the partner country into the Polish system, increased employment mobility, and language skills.

The Inspector General and Direct Marketing Association signed the agreement on cooperation aimed at improving personal data protection level as well as ensuring that citizens have the right to privacy in the direct marking sector.

Educational activities play a particular role in the tasks of the Inspector General for Personal Data Protection. It was implemented *inter alia* through broad cooperation with media. In 2008, the Inspector General gave about 100 interviews in which he presented his standpoints or commented upon and clarified different data protection issues.

Portugal

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

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

The Directive 2006/24/EC (Data Retention Directive) was transposed into national law by Law 32/2009, entering into force in August 2009. The legislative procedure was initiated in 2008, and the DPA was asked by the Government, and later by the Parliament, to provide Opinions on the draft law. The considerations and suggestions made by the DPA were very much taken into account in the final text. The maximum retention period was set to one year. The crimes for whose investigation the traffic data can be used are specified in the law, as well as the obligation for judges to directly request the data from telecom service providers upon justification. A list of the staff authorised to have access to the traffic data, for purposes of the law, has to be communicated to the DPA, as well as regular reports on the data retrieved. The communication between the judges and the telecom service providers is made online through a particular form.

B. Major case law

None to report.

C. Major specific issues

General activity
The Portuguese DPA substantially increased its activity during 2008. The number of data processing notifications has doubled to ten thousand.

To face this huge amount of work, the DPA is taking measures to make the decision-making process easier and faster, although not to the detriment of any in-depth analyses required in the case of some issues.

The DPA is changing its information system, created and developed by our own IT staff, to adapt it to the ongoing dematerialisation of internal procedures, in order to abolish hard copies in the future.

While the DPA is also developing the electronic notification procedure for all kinds of data processing, in order to ease the procedure for data controllers and speed up the permits, in 2008 it started two specific e-notifications, as part of a fully automated procedure, for a video surveillance programme in schools and for the processing of sensitive data in the area of child victim support.

Another important aspect of the DPA activity is to provide guidance to and to raise awareness of both data controllers and data subjects. In addition, the increasing participation of the DPA in public seminars and conferences concerning data protection in different sectors, should be highlighted.

Opinions on draft laws
The DPA was asked to provide 59 Opinions on draft laws containing data protection matters. The most relevant concerned the transposition of Directive 2005/60/EC on money laundering and the fight against terrorism, the population census, the amendment of the electoral roll database, data processing in the judicial system, amendment of the Labour Code and vehicle event records. Within its competences to issue Opinions, the DPA was also heard by the Parliament regarding draft laws.

The issue concerning the implementation of what is known as "vehicle plate electronic device" caused much public discussion, with the DPA acting as a reference for the debate, as it raised concerns on this project. According to the draft law, the device will be mandatory for all vehicles and will have multiple purposes: to allow law enforcement authorities to detect traffic infringements (such as lack of insurance, apprehended driving licence, or unpaid fines) and to allow the payment of tolls in Portugal, as well as in the European Electronic Toll System. The technology chosen was the DSRC, which has a range of 1000 metres.

The DPA raised two main questions in relation to the draft law: although the technology to be used would

be less intrusive than the GPS options, it has yet to be decided how many readers would be installed to prevent the possibility of tracing a vehicle's route; on the other hand, since the device is mandatory on all vehicles, it should always be possible for the driver to pay the toll anonymously without leaving an electronic trace of his whereabouts.

The law was approved by the Government last February, and it has been decided that, for the time being, this device is only going to be used as a means of toll payment. The other purposes were excluded. There is still some regulation to be done and the DPA will have to be involved in the process, as well as in subsequent data processing authorisations.

DADUS Project

In January 2008, on European Data Protection Day, the Portuguese DPA launched a pioneering project called the DADUS Project, to introduce data protection matters into school curricula, side by side with other subjects, following an Agreement with the Ministry of Education and the Education Regional Authorities for Azores and Madeira.

The goal is to raise awareness on data protection rights and provide guidance to young people on how to use ICT in a more secure way, and in particular, to achieve it through a structured, nationwide and long-term project that goes further than a simple occasional campaign.

This Project targets children from 10 to 15 years old and its contents are based on Internet platforms. The DPA developed a dedicated site for the Project, where teachers are provided with a basic data protection manual with several supporting materials to work in the classroom, and a blog for the interactive participation of pupils, with games, tips, texts, school work, pupils' comments and cartoons, either at school or at home.

The DADUS Site also contains a special area for parents, with simple and clear information on data protection, allowing them to monitor their children, and a discussion forum to exchange experiences and share doubts and solutions.

Last year, the focus was mainly on presenting the Project to schools and distributing some printed materials to teachers. The first reactions were very positive and many teachers immediately adhered to the Project in the 2007-2008 school year, even in private schools. In the first year of the DADUS Project, there were already around 1 700 teachers registered in the Project, and the Site and Blog had achieved more than 100,000 hits.

Romania

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

Directive 95/46/EC of the European Parliament and Council has been transposed into Romanian legislation through Law No 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, adopted on the 12 December 2001.

Law No 677/2001 has been modified by Law No 102/2005 on the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing. The most significant modification refers to the abolition of the provisions on the need to obtain a preliminary agreement of the criminal investigation body or of the competent court of law in the cases in which the Supervisory Authority intended to carry out an investigation in relation to personal data processing carried out in the field of criminal law.

Another modification of Law No 677/2001 has been carried out by Law No 278/2007 in the sense that the notification fee for personal data processing under the scope of Law No 677/2001 has been abolished.

No further modifications have been made during the course of 2008 to the Law on the protection of individuals with regard to the processing of personal data and the free movement of such data.

Directive 2002/58/EC on the processing of personal data and the protection of private life within the electronic communications' sector has been transposed into national law through 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 providers of public electronic communications' networks, the providers of added value services, as well as the providers of subscribers' records. This law amends and specifies the legal framework established by Law No 677/2001, within the specific sector of electronic communications.

Directive 2006/24/EC has been transposed into national legislation through Law No 298/2008. The objective of this law was to provide a national regulation on the obligations of providers of public communication networks and services to retain data generated or processed in relation to their activities for a period of 6 months from the date the electronic communication was made, in order to make the data available to the competent authorities in the context of activities of criminal investigation and prevention of criminal offences.

In 2008, bearing in mind Romania's status of an EU member state, the supervisory authority took into account, within its regulatory activities in the field of personal data protection, the specific issues observed in its daily activities. The following decisions have therefore been adopted: Decision 90/2008 on the adequate level of personal data protection in Jersey, Decision No 95/2008 on establishing the standardised notification form, provided by Law No 677/2001, Decision 101/2008 on the processing of personal data referring to state of health and establishing an authorisation model for processing the personal data referring to state of health.

In order to accelerate the national legislative procedures on the implementation and harmonisation of the community's *acquis*, which are applicable in various fields of activity, the Supervisory Authority has collaborated constantly with national institutions by providing expert opinions on certain legislative acts during their adoption procedure. In this respect it is worth mentioning the following: Draft Government's Decision on the procedure of authorisation of providers of public services of electronic authentication, Draft Government's Emergency Ordinance on the modification and amendment of the Law on the regime of free circulation of Romanian citizens outside Romania, Draft Government's Emergency Ordinance on regulating the use of personal data in the police sector – transposition of Recommendation 87 (15) of 17 September 1987 of the Council of Europe's Council of Ministers.

The Supervisory Authority has also issued numerous opinions, points of view, recommendations and

instructions in accordance with the principles and provisions established in both community and national legislative acts on processing personal data.

B. Major case law

It was noted that in 2008 the courts of law adopted a standard practice in the litigations related to personal data protection.

Despite the diverse nature of the issues contested before the courts of law and of the situations submitted for judicial control, the legislation on personal data protection has been interpreted in a similar manner to that of the supervisory authority

In this way, following the Supervisory Authority's investigation at a private company, it has been noted that the company processed personal data via e-mail messages and a fine was imposed for transmitting unsolicited commercial communications through electronic means. The data controller formulated a complaint against the investigation report

In view of the evidence submitted in this case, the court of law ascertained that the data controller processed the personal data of the individuals to which it had transmitted the commercial communications without the recipient being able to exercise his or her right of opposition. More specifically, the recipient received repeated commercial communications without any prior consent to receive such communication.

In view of these findings the court of law decided that the Supervisory Authority had correctly determined the minor offence committed and the fine that it imposed was legal.

As part of an investigation at a sports club, the Supervisory Authority noticed that it had processed both manually and automatically the personal identification number, first name and surname of supporters that had purchased subscriptions, without any prior notification of that processing of personal data and without providing any information to the data subjects with regard to their legal rights.

The Supervisory Authority sanctioned the data controller for failure to notify the processing of personal data of its supporters, as well as for the lack of information which should have been provided to the data subjects with regard to their rights and the ways in which those rights could be exercised.

As a result of the fine, the data controller issued a notification regarding its personal data processing and provided the information required by Law No 677/2001.

C. Major specific issues

The control activity of 2008 focused on carrying out the investigations as per the yearly plan, as well as investigating possible illegal processing of personal data pointed out within the complaints and notices received by the Supervisory Authority.

The majority of *ex officio* investigations have been based on the yearly investigation plan set up on issues derived from the Authority's activities, in fields of activity where previous infringements of Law No 677/2001 and the submission of few notifications had been noticed.

More specifically, whilst carrying out the yearly investigation plan, four major fields of activity were monitored:

- SWIFT
- Healthcare and maintenance centres
- Online commerce
- Video surveillance

SWIFT –it was decided that certain **ex officio** investigations must be included within the yearly investigation plan as a result of various issues raised within the Article 29 Working Party, more precisely the control of personal data processed within the system for international financial transactions - SWIFT.

In continuation of its monitoring and control activities as established by Law No 677/2001, the Supervisory Authority has verified the observance of the legal obligations imposed upon financial institutions by the transfer of data within SWIFT transactions to the USA

and, at the beginning of 2008, verified the fulfilment of their obligation to inform the data subjects.

The investigations showed that the data are transmitted to SWIFT operational centres based on a standard contract between each participant and SWIFT; the contract provided for similar clauses for all participants and therefore ensured standard practice as regards the way in which personal data were processed and transmitted to SWIFT operational centres.

As regards the information of data subjects with regard to the transfer of data via SWIFT, as a way to provide information, the banks posted information notices at their premises and on their websites, which included information on the possibility of transmitting to US authorities, upon their request, personal data related to transactions carried out via SWIFT after 11 September 2001. The information notice also contained information on the fact that the US Finance Dept. is able to request access to the personal data of bank customers stored in SWIFT's operational centre exclusively for purposes of combating terrorism and that the personal data were stored only for as long as required for that purpose and stored in a secured environment.

The verifications carried out revealed that some data controllers had not issued any notification regarding the processing of personal data for those purposes and that some financial banking institutions did not provide adequate information to the data subjects as provided by Article 12 of Law No 677/2001. As such, they have been asked to resolve these deficiencies.

The data controllers have followed the recommendations of the Supervisory Authority.

Healthcare and maintenance centres – The verifications carried out during investigations showed that not all data controllers issued notification regarding their processing of personal data before this was initiated

Example: Company X was sanctioned for failure to notify as it had not issued notification of the processing of personal data it carried out in order to provide goods and services prior to the beginning of processing operations, and for illegal processing of personal data as no information had been provided to data subjects as regards their legal rights.

A recommendation was made in the investigation report for the data controller to issue notification of its processing of personal data, to inform the data subjects of their legal rights and to sign confidentiality clauses with staff members that have access to personal data.

As it had been noticed that the company also processed the customers' personal identification number and their bank account number, a decision was issued to stop the processing of the personal identification and bank account numbers, as this was considered to be excessive in relation to the purpose of the processing to "provide goods and services" and "advertising, marketing and commercials" and to delete the data processed before this decision.

Further checks performed in this case proved that the data controller had observed the measures imposed through the investigation report – as it had stopped processing the personal identification number and bank account number for the purposes of "providing goods and services" and "advertising, marketing and commercials" and deleted the data processed up to that point.

Following the investigations carried out within this specific sector, the number of notifications submitted by data controllers has increased significantly, which indicates an increased awareness as regards their obligations related to personal data protection.

Online commerce– In consideration of the fact that this activity implies the processing of personal data of individuals, including sensitive data (e.g. personal identification number, series and number of identity documents), as well as the risks entailed by the collection of such data on the Internet, the Supervisory Authority has carried out several investigations at private companies that perform such activities.

The sections "Terms and conditions" and "Confidentiality Policy" posted on the data controllers' websites contain information providing reasons why the personal data are collected and stored, including the fact that the

data will not be further disclosed to third parties. These documents did not, however, contain any information on the rights granted to the customers by Law No 677/2001.

The checks performed revealed that most data controllers had not issued any notification regarding the processing of personal data carried out for that purpose prior to the investigation, but did observe that obligation thereafter.

Example: An investigation, carried out in 2006 at a company whose activity consisted of online sales, revealed that the data controller processed, via its dedicated website, the personal information of those who were interested in the company's offers and those of its customers (natural persons) and maintained records of those data, both electronically and on paper, which fell under the scope of Law No 677/2001. The individuals were asked to provide, via the online form, personal data such as: first name, surname, personal identification number, delivery address, e-mail, and phone number. According to the declarations made by the company's representatives, it was not compulsory to provide a personal identification number in order to issue an invoice and no further grounds were provided in favour of collecting this type of data.

Moreover, in the "Terms and conditions" section, the website contained an information notice which indicated the categories of data subjects (customers - natural persons), but no reference to law No 677/2001 or the rights of the data subjects and the ways in which those rights may be exercised in accordance with paragraph (1), Article 12 of Law No 677/2001.

In view of the issues observed during the investigation, the data controller was sanctioned for failure to issue notification of the processing of personal data and for illegal processing of personal data as they did not provide adequate (complete) information to the data subjects.

Following the investigation it was noted that the order form posted on the website had been changed and provision of the personal identification number was no longer compulsory.

Based on the investigation's findings, the Supervisory Authority issued a decision through which it imposed the deletion of the personal identification numbers stored in the company's database, as the data controller did not indicate a determined, precise and legitimate purpose justifying the processing of the personal identification number, in accordance with the provision of articles 4 and 8 of Law No 677/2001.

The data controller is now in compliance with the measure imposed by the Authority.

Video Surveillance – the supervisory authority has received, during the course of 2008, a large number of notices relating to checking the observance of the obligation to notify by various public and private bodies which used video surveillance means.

As a result, the supervisory authority carried out a series of investigations in relation to the processing of personal data through video surveillance means, *ex officio* or after receiving complaints or notices from data subjects.

Whilst carrying out these investigations the following main issues were monitored: observance by data controllers of the minimum security measures, establishment of a legitimate and explicit purpose, prevention of excessive storage of personal data processed through means of video surveillance, granting the data subject the possibility to exercise his or her rights (granted by law), and avoiding any disclosure of data processed in this way without legal grounds.

The justification provided by data controllers for installing video surveillance cameras was the prevention of thefts and other illegal activities. The collected images are stored on servers for a certain period, depending on the capacity of the storage unit, after which they are deleted automatically. The images are disclosed to police bodies only when criminal offences are committed and only on the basis of an official request.

Example: The data controller, investigated after receiving a notice, processed personal data, namely images obtained through video surveillance cameras installed in a restaurant.

The investigation revealed that the cameras were also installed in the toilets and enabled individuals to be identified. The purpose declared by the data controller for the surveillance system was to ensure the "security of premises and goods and prevention of criminal offences".

The warning with regard to the video surveillance was only posted at the restaurant's entrance.

As the data controller had not notified that it was processing of personal data, he was fined for failure to notify and for ill-intended notification.

Following the investigation and bearing in mind that the toilets are a private space reserved only for the individuals that use them at any given time, the Supervisory Authority considered that installing the video surveillance system in these rooms was excessive, following the same lines expressed by the Article 29 in WP 67/2002 on the processing of personal data through video surveillance means.

In view of the issues mentioned above, the Supervisory Authority issued a decision to stop the processing of images of individuals that use the restaurant's toilets and to delete the data collected up to that time.

In the case of video surveillance systems installed in order to accomplish the obligations imposed by Law No 4/2008 on the prevention of violence at sporting events, the Supervisory Authority undertook investigations at major football clubs in Bucharest and in other cities. The findings showed that in the majority of cases no notification of processing of personal data (images) was given before such processing was initiated and, as such, the data controllers were fined.

Furthermore, in most situations, the data controllers had taken steps to ensure the information of individuals with regard to the video surveillance means used in football stadiums, both by means of written notices posted in visible spots and through verbal warnings issued during the sporting events.

During the course of 2008, in addition to the approved plan, investigations were also carried out in the following areas:

- The national programme for evaluation of the population's state of health in primary medical care – the processing of personal data within this programme, and
- The Diagnosis Groups Classification System (DRG) – processing of patients' personal data.

Following the investigations, there has been a significant increase in the number of notifications received from data controllers whose activities fall under the scope of supervision of the NSAPDP.

The resolution of complaints derived from the Supervisory Authority's activities is an extremely important issue. In 2008, the number of complaints received increased by a factor of 11 compared to 2007, which clearly demonstrates that the Supervisory Authority's powers and the field of personal data protection are much better known by the general public and that citizens are showing an increased interest in our authority's activities. The majority of complaints referred to receiving unsolicited commercial communications, reporting personal data of debtors to the Credit Bureau and the Banks' Risk Centre, and the illegal disclosure of such data in other situations.

Slovakia

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

A minor, but very important change in the area of legislative regulation governing the factual existence and functioning of the Office for Personal Data Protection of the Slovak Republic (hereafter referred to as „the Office") has been performed. Through this specific change, Act No 428/2002 Coll on Protection of Personal Data (hereafter referred to as "Act No 428/2002 Coll") has been amended regarding the "Personal Data Protection Budgetary Program" which was transferred from the budgetary category of the Government Office of the Slovak Republic to the General Treasury Administration category. This transfer has formally strengthened the independence of the Office in the budgetary field. In the next budgetary year it will not be necessary to submit the budget for approval as part of the Government Office's budget. This legislative amendment , however, still leaves in the possibility of ignoring financial requirements of the Office because the General Treasury Administration category is under the administration of the Ministry of Finance of the Slovak Republic whose budget is submitted for the negotiation and approval of the National Council of the Slovak Republic.

B. Major case law

In 2005, the Office issued an order requiring the state administrative authority as a controller of the filing system to terminate the disclosure of national identification number (an identifier of general application) of data subjects on the website of the Official Journal. The controller was also instructed to remove previously published national identification numbers from its website. Recipient of the order filed with the Office the objection against this decision. His objection was rejected as unacceptable. The controller filed a petition with the court whereby he requested the cancellation of the Office's decision. The court dismissed the claim and in its opinion stated that making personal data public is a very specific processing operation. A particularity of this operation lies mainly therein that it is a process which cannot be absolutely undone (restored as if nothing had ever happened) and brings about all range of consequences, which may have, in the case of unlawful disclosure, a negative effect on data subject. The disclosure of national identification numbers is even more sensitive. Finally, the law explicitly prohibits the disclosure of "identifier of general application". According to the court, the decision of the Office was based on appropriate grounds and was in line with the competence granted to the Office by law.

C. Major specific issues

Inspection activity and issue of notifications

Department of Inspection of the Office executes an independent supervision of personal data protection and by performance of its activities strengthens the protection of other fundamental rights and freedoms of natural persons. Activities of the Inspection's Department are mainly focused on the inspection of filing systems of controllers and processors and handling of notifications of data subjects and other individuals who claim to have been directly aff ected in their rights stipulated by Act No 428/2002 Coll.

Supervision of personal data protection in figures

In 2008 data subjects and other natural persons who claimed a breach of the protection of their personal data filed 113 notifications with the Office. A further 65 notifications were filed by other subjects who alleged the suspicion of violation of the Data Protection Act. The Chief Inspector of the Office ordered 74 proceedings against the controllers of filing systems to be conducted *ex officio*. Another 21 notifications were pending from the year 2007. Overall, the inspection department in 2008 dealt with 273 notifications. In this regard the Inspection's Department by the controllers and processors of filing systems conducted 105 inspections and 34 "submissions to explanations". Altogether 75 orders were issued for removal of deficiencies determined by the inspection. The right to file an objection against the issued order had been used only by one controller. Objection was dismissed.

In 2008, 142 out of 252 new notifications were filed against private sector controllers, 61 against controllers from public administration, mainly against the other public administration bodies. In 28 cases, the Office investigated notifications against self-government authorities.

Eight cases related to the civil society organisations, foundations, political parties or movements and registered churches or religious groups. Public administration institutions were investigated in 4 cases. In 9 cases, the notification was filed against a subject who was not the controller of the filing system under Act No 428/2002 Coll.

Out of the 113 notifications filed by data subjects in 2008, the Office completed 99 cases, of which 71 were accomplished within the basic statutory period of 60 days. Longer investigation of other notifications was caused by the need to consult other institutions, inspections of filing systems at a controller's premises, to gather more evidence or by the request to cooperate presented by the petitioners. A total of 50 of all handled notifications were evaluated as being without grounds.

If an informant is not satisfied with addressing of his notification by the Office, he can repeatdly submit to the Office a notification within the statutory period of 30 days. Out of the 99 completed cases in 2008 only 2 repeat notifications were submitted to the Office. Remaining 97 informants whose notifications have been examined in 2008 respected the final decision of the Office which is more than 96 %. During 2008 the Department of Inspection passed 4 notifications to the law enforcement agencies.

In 2008, the Office imposed 14 fines for a total amount of 1 045 000 SKK (€34,687.65). Sanctions usually have fallen in the lower-bound of possible rates as the Office disposes of a margin for manoeuvre in regard to imposing of fines. The maximum penalty imposed was 250,000 SKK (€8298.5).

Nationwide inspection activities of the Office

Inspections of video surveillance systems in towns and municipalities

In 2008, the Department of Inspection carried out inspections of video surveillance systems. The nationwide inspection was aimed at examining the video surveillance systems operated by towns and municipalities. The Department of Inspectionthus conducted 12 inspections, 7 of which took place in 2007. Deficiencies were noted during all conducted inspections. The Office therefore issued orders to the controllers. The most common shortcomings lied therein that the monitored areas which are accessible to the public were not clearly marked as being monitored, they did not keep records of the filing system, failed to destroy the recordings within the period stipulated by Act No 428/2002 Coll and they failed to take due technical, organisational or personal measures in the form of security directive for camera filing system.

Inspections aimed at the processing of personal data by executors, notaries and attorneys

In 2007, it was noted that several executor offices stepped outside the framework of the provisions of Act No 428/2002 Coll by disclosing the national identification numbers of data subjects on the official notice board (announcement of the initiation of execution, auction notice). The inspections of executor offices carried out in 2008 also revealed shortcomings in the application of provisions of the Act No 428/2002 Coll related to security of the processing of personal data, especially in those cases where the filing system processing the personal data is connected to Internet.

The Department of Inspection checked the status of compliance with the provisions of Act No 428/2002 Coll at selected notaries and law offices throughout the Slovak Republic.

In particular, the following were examined:

- advising of entitled persons;
- content of contracts between controllers and processors;
- keeping records of human resources and payroll filing system and client's information system;
- authorisation of a personal data protection official;
- existence and quality of a security project or security directives.

The orders were issued in order to eliminate shortcomings and after an in-depth analysis of the whole case discussed by the Chief Inspector with the competent representatives of the Slovak Bar Association, Slovak Chamber of Executors, Chamber of Notaries of the Slovak Republic who from their position can effectively provide the competent subjects with guidance on how to remedy their situation as soon as possible.

Inspections aimed at processing of personal data by the controllers in the healthcare sector

In 2008, the Office dealt with several notifications from data subjects against the controllers in the health sector. As the number and importance of some of those notifications was critical, the Chief Inspector decided to carry out inspections to check to what extent the controllers in the healthcare sector complied with the provisions of Act No 428/2002 Coll regarding the processing of patient's personal data. The Department of Inspection inspected state and private healthcare facilities (hospitals and surgeries), pharmacies and health insurance companies. In most cases, controllers had failed to provide security directives which would clearly define the scope of competence and description of functions of entitled persons and the scope of their responsibilities in relation to what kind of operations those persons do with the personal data, even during some extraordinary situations (e.g. closing or moving a surgery or hospital). In several cases, the Office noted that personal data were being obtained or disclosed in an indiscreet manner in healthcare facilities and pharmacies. In addition, suspicions of leaked personal data regarding newborns to the health insurance companies were handled by the Office.

Special inspection activities carried out in relation to the accession of the Slovak Republic to the Schengen area

In relation to the preparations for accession of the Slovak Republic to the Schengen area, the Department of Inspection pursued in 2008 further inspections in the selected embassies of the Slovak Republic abroad. Its aim was to examine compliance of the controllers of filing systems with Act No 428/2002 Coll, procedures applied while issuing Schengen visas and fulfilment of the requirements stated in the Schengen catalogue (recommendations and best practices) related to visa issuance. In March 2008, the consulate departments of the Slovak Republic embassies in Kuwait and Damascus were inspected and, in May 2008, consulate departments were inspected in Prague and Brno. With regard to monitoring of legal processing of personal data in accordance with the present version of Schengen Information System (SIS I) the inspection was conducted at the National Office of SIRENE, the Office of International Police Cooperation and in the Presidium of the Police Force.

International cooperation

The Office regularly participates in spring and autumn international workshops for inspectors of the personal data protection authorities. At the autumn workshop in 2007, which was organised by the Portuguese authority for personal data protection in Lisbon, it was decided that the XVIII International workshop for inspectors in autumn 2008 would take place in Slovakia. The workshop organised by the Office was held on 29 to 30 September 2008 in Bratislava. In addition to the inspectors from the Member States of the European Union, the workshop also received inspectors from candidate countries, which are preparing to join the European Union. Overall, 63 foreign participants and 10 of the Office's employees took part at the workshop. The European Data Protection Supervisor's Office was represented by two delegates. The event was opened by the Chairman of Parliamentary Committee on Human Rights, Minorities and the Status of Women and by the President of the Office. At the meeting, the inspectors dealt with five basic themes during the following panels:

1. Complaints handling: powers of supervisory authorities in the handling of complaints;
2. Exchange of best practices from the inspections at the consular departments of the embassies regarding Schengen visa issuance;
3. Balancing of interests: Personal data protection vs. mass media;
4. Application of security measures in the processing of personal data;
5. Processing of personal employment data.

Department of Inspection presented the topics as follows:

- Performance of inspections and internal rules for inspection;
- Provision of explanations and personal data protection official;
- Entitled person; organisational and personal measures;
- Legal framework and conditions for the preparation of a security project;
- Legal framework for processing personal data by a video surveillance system and the experience of the Office in the exercise of inspections of video surveillance systems.

Cross-border Personal Data Flow

During the monitored period the Office issued 3 approvals of the trans-border flows of personal data. The subjects of the trans-border data flow were personal data processed in the employment context, human resources management and outsourcing of processing operations. One decision on cross-border transfer to countries that do not provide an adequate level of personal data protection was issued to the controller – importer based in India on the basis of compliance with legal provisions stipulating the need to incorporate standard contractual clauses in the contract. Two decisions on transfer of personal data were issued by the Office for importers in the USA following the self-certification of importers in the Safe Harbor. On the basis of documents received, it was clear that the controllers did not know how to properly use and interpret the relevant decisions of the European Commission, which were issued in order to provide sufficient safeguards for the protection of personal data by and after their transfer to the third countries. The Office also dealt with requests for "special registration" of system for reporting suspicions of unlawful or unethical action (whistleblowing) and related requests for the approval of the transfer of such data to processors in the USA. The Office also provided several opinions interpreting Act No 428/2002 Coll and the opinions of Article 29 Working Party with respect to this issue. In the monitored period, the Office issued one decision rejecting the special registration based on processing data provided through whistleblowing. After the removal of identified deficiencies, the Office eventually allowed "special registration" in that case. With regard to whistleblowing, no transfer of such data to third countries was permitted by the Office. After examining the applications for approval of the transfer of personal data, the Office came to conclusion that they did not contain the facts necessary for granting an approval on the matter concerned. Those widely designed whistleblowing systems went far beyond the scope of the Act No 428/2002 Coll. In this respect, it related solely to whistleblowing systems developed abroad, which were already set up and had been operating for an extensive period.

International cooperation

Bilateral meetings are held for the purpose of addressing particular issues, arranging cooperation or for the exchange of best practices. Those meetings are attended by the president of the Office and competent experts.

May 2008 – Bilateral meeting with the Personal Data Protection Office of the Czech Republic convened by the Slovak Office and taking place in Slovakia. Topics of the meeting were the issues giving rise to the exchange of best practices on the performance of inspection activities:

- Use of official documents in practice: identity card and passport as European documents. Legislation concerning official documents; the scope of personal data in official documents
- Processing and disclosure of personal data from central registers (filing systems) of the Ministry of Justice of the Slovak Republic regarding jurisdiction (e.g. Official Journal of Court Decisions, Collection of Documents)
- Exercise of inspection at the controlled subjects' premises (controller/processor) without the need to give notice. Cooperation of the state administration authorities and other public administration bodies with the DPA in the Slovak and Czech Republic.

April 2008 – Visit to the Office of the General Inspector for Personal Data Protection in Warsaw, Poland.

The purpose of the visit was to become familiar with the organisational structure and activities of the Polish DPA (GIODO). On this occasion presidents of the both DPAs gave an interview to the daily newspaper "Rzeczpospolita".

April 2008 – Visit to the National Office for Personal Data Protection in Bucharest, Romania.

The programme of the visit was linked to the previous bilateral meeting in Bratislava dealing with the topic of Romania's preparation for accession to the Schengen area. The programme was extended to the exchange of best practices, which were for instance related to the particularities regarding the independence of the Romanian DPA.

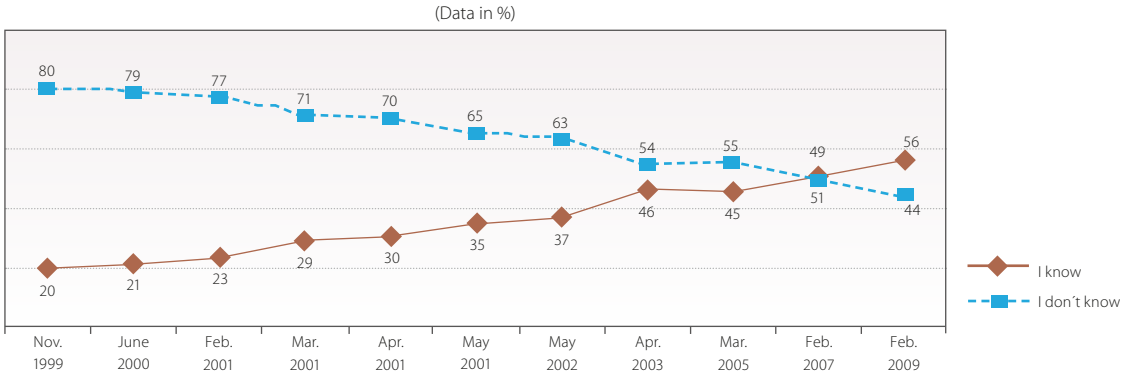
Public awareness of personal data protection

The Opinion Research Institute of the Statistical Office of the Slovak Republic has repeatedly conducted a public opinion poll since 1999, at the instruction of the DPA, on questions related to personal data protection. The last survey was carried out in February 2009.

As can be seen from the graph, during the last two years - from February 2007 to February 2009 - the awareness of all categories of citizens personal data protection rights increased by 5 %. Altogether - from November 1999 to February 2009 – it has risen by 36 %.

Generally, it can be stated that the highest awareness (higher than average for the whole Slovak Republic) is shown by citizens aged from 30 to 39 years (68 %), 40 to 49 years (66 %), respondents with a university degree (87 %), respondents who have completed secondary education (67 %), as well as businessmen (70 %), employees (74 %), and citizens of cities with over 100,000 inhabitants (76 %).

Do you know your rights on protection of personal data resulting from the Act No 428/2002 Coll on Protection of Personal Data?



Slovenia

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

Through the adoption of the Personal Data Protection Act[21], the Information Commissioner Act[22] and the establishment of the Information Commissioner[23] as an independent data protection authority, Directive 95/46/EC has now been fully implemented into the Slovenian legal order.

Authorised by the special provision of Article 48 of the PDPA, the Information Commissioner issued several preliminary opinions on legislation in preparation regarding compliance of personal data protection. The major pieces of legislation considered in 2008 were the laws on personal identity cards, aliens, judicial register, electronic communications, as well as various regulations in the areas of public health and health insurance, free-of-charge legal aid, etc.

In the line of his duties, the Commissioner has encountered a problem regarding acquisition of mobile phone location data in cases when an individual's life or body is endangered not in connection to criminal proceedings and the police require the location data upon receipt of emergency call. In this context, the Commissioner has suggested that amendments be made to the Electronic Communication Act[24]. According to amendments proposed, the police in the described situation would have the right to request the data about the last known location of the mobile device carried by an individual whose life or body are at risk. The police would retain this documentation permanently, and the Commissioner would perform supervision on data retention at least once a year. This amendment also appropriately implements Article 5 f of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[21] Adopted in 2004, amended in 2007 (Official Gazette of the RS, No 94/2007 – Official consolidated text), hereinafter: PDPA.

[22] Official Gazette of the RS, No.113/2005.

[23] Started operating on 1 January 2006.

[24] Started operating on 1 January 2006.

B. Major case law

In 2008, the Information Commissioner dealt with several **cases widely publicised** by the national media.

Telephone communication traffic data misused by foreign ministry

The Information Commissioner issued a regulatory decision in a case against the Ministry of Foreign Affairs regarding the lawfulness of the processing of personal data by means of acquiring a copy of telephone numbers from a fixed telephone network including those numbers which had been dialled as well as those numbers from which incoming calls had been made. The Ministry was ordered to destroy the CD on which the related list of telephone numbers was stored.

For the purpose of the internal investigation within the Ministry and with the aim of identifying the employee who handed over a diplomatic mail to a journalist of the daily newspaper all traffic data from a certain period were collected. Thus a database was created containing approximately 110,000 items of traffic data.

In accordance with the Electronic Communications Act the traffic data are granted double protection, namely the protection of the privacy of correspondence and other means of communication according to Article 37 of the Constitution of the Republic of Slovenia (hereinafter: Constitution) and also the protection of personal data according to the Article 38 of the Constitution. Since traffic data are considered to be personal data as they relate to an identified or identifiable natural person, in a case of illegal intervention such as this, there is a double violation of rights, namely on the side of the employees of the Ministry as well as on the side of all those called by the employees or who dialled the latter's telephone numbers.

In accordance with paragraph one, Article 37 of the Constitution, privacy of correspondence and other means of communication is ensured. Paragraph two of this article stipulates that only a law may prescribe that on the basis of a court order the protection of

the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where this is necessary for the institution or course of criminal proceedings or for reasons of national security. The extent of protection of the communication privacy as defined by Article 37 of the Constitution originates from the need for protection of privacy of relationships into which an individual enters during communication, and not from a certain type, status or ownership of the medium or communication means. This protection is granted to all persons, as the Constitution does not differentiate between privacy in the private or official sphere.

The Information Commissioner stated that the Ministry acquired and used the data for the inadmissible purpose of investigating the traffic data to establish which employees called the newspaper. Additionally, from the point of view of the principle of proportionality, the case of a clear lack of proportionality was established as by virtue of the acquisition of the aforementioned traffic data, no evidence has been found that someone actually leaked a specific document.

Competition Protection Office

The Commissioner decided that it was prohibited for the Competition Protection Office (CPO) to further process personal data contained in the copies of personal computer hard drives acquired while conducting the procedure to find out whether the biggest three Slovenian retailers had been involved in coordinated actions.

During the inspection procedure, the Commissioner stated that Article 29 of the Restriction of Competition Act does not provide sufficient legal basis for accessing the electronic correspondence and related traffic data. According to the strictness of the Constitution (Article 37), the Act does not specify processing of e-mails as a form of investigation and access to e-mails would therefore mean an intrusion into constitutionally provided communication privacy. The Commissioner instructed the CPO to block access to the acquired electronic files which also contain illegally acquired personal data and within five days transfer from the media containing the electronic files the parts that may still be used in further investigation. Each access to the acquired media shall be performed in the presence of the Commissioner. In a judicial review of the decision, the Administrative Court rejected the request by the CPO to be permitted to investigate personal data on the copies of hard drives until the legal decision is final and thus sustained the Commissioner's decision. The Supreme Court denied CPO any judicial protection as an administrative body in the administrative dispute procedure since the competencies and mandates of an administrative body in performing its administrative tasks cannot be regarded as rights or benefits that a court would protect through the administrative dispute procedure.

Protection of sensitive personal data

The Commissioner has dealt with serious cases of inappropriate protection of sensitive personal data. During transport to the place where the data (orders for laboratory examinations) were supposed to be destroyed, cardboard boxes containing the data fell out of the truck and caused the data to be scattered across the motorway. The data controller – a primary healthcare centre – had entrusted the transport and destruction of files containing personal data to a contracted data processor, registered for performing activities of waste collection and transport. The healthcare centre, however, had not arranged mutual obligations regarding data processing by contract, which it should do according to PDPA. It had not given appropriate instructions as to the protection of data during transport and destruction, nor had it supervised the execution of procedures and measures for personal data protection by the contracted processor. Due to inappropriate protection of personal data and non-compliance with the statutory provisions regarding contractual processing of personal data, the Commissioner fined both the data controller (the health centre) and the processor – the company contracted to transport and destroy the documentation.

Another widely publicised case of inappropriate protection of sensitive personal data was uncovered during inspection supervision of the Institute of Oncology. The medical documentation – medical files containing data on deceased patients – was found to be stored in more than a hundred open, unprotected cardboard boxes placed in the corridor. Additionally, in the same widely accessible corridor, two cabinets

were placed containing partial documentation on patients currently receiving medical treatment. The data controller which should have protected the data appropriately according to statutory provisions on sensitive data was fined by the Commissioner.

The Mayor
The Mayor of one of the Slovenian municipalities was delivered an initiative by the voters regarding a call for referendum on construction of residential buildings in the municipality. Initiative appendices included a list of more than 400 voters who had signed the initiative and enclosed their personal data for that purpose. The Mayor handed over a copy of the initiative to the lawyer hired by the company which was to construct the residential buildings. The lawyer later on used the personal data from the list of signatories for a purpose different from that for which the data were collected. Namely, the lawyer notified the signatories of the initiative that a claim for damages had been initiated against them and called for them to retract the signature on the initiative. Both the Mayor and the lawyer were fined for unlawful processing of personal data.

Tax Administration of the Republic of Slovenia
The Commissioner has also been supervising protection of personal data by the employees in different registers of public administration, namely the justifications for access to the central register of taxpayers. According to the PDPA data controller, in this case the Tax Administration of the Republic of Slovenia was obliged to enable subsequent determination of when personal data were entered into the filing system, used or otherwise processed. Thus the Commissioner was able to investigate all access to the computer base of taxpayers related to 15 publicly well-known persons from Slovenia. The Tax Administration handed over to the Commissioner a list of employees who accessed the data of the aforementioned 15 persons within a period of 8 months in 2008. Each of the employees was requested to justify the processing of the data and it was determined that only 47 out of 200 employees had accessed the data lawfully, namely for the purpose of conducting a taxation procedure. The rest of the employees had no justifiable reason for accessing the data. Curiosity was named as the most common reason for access to public persons' age or address data. The Commissioner issued warnings to the civil servants who accessed the data without sufficient legal basis as a lesson that personal data may not be accessed without lawful justification.

Review of the constitutionality
Based on the provision of Article 23a of the Constitutional Court Act authorising the Information Commissioner to initiate the procedure for the review of the constitutionality or legality of regulations if a question of constitutionality or legality arises in connection with a procedure he is conducting, in 2008 two further requests for constitutional review of certain provisions of the Banking Act and the Slovenian Intelligence and Security Agency Act were lodged. The former case which relates to the provision of the Banking Act on compulsory establishment of the information system on credit standing of the clients and on compulsory contribution of respective information by the banks was withdrawn in March 2009 due to successful negotiations with Ministry of Finance to amend the law, namely to list the data which needs to be stored in the system and for how long.

Regarding the inspection supervision of the Slovenian Intelligence and Security Agency, the Commissioner lodged a request for constitutional review of the Slovenian Intelligence and Security Agency Act, a review of the provisions regarding the strategic telecommunications supervision, which implies emergence of personal data filing systems. The Commissioner requested that the Constitutional Court determine the discrepancies between certain provisions of the Act and Article 38 of the Constitution (basic human right to data protection or information privacy). The Commissioner also requested that the Court determine whether the provisions of the Act were in accordance with Article 37 of the Constitution which provides for communication privacy and defines the conditions and limitations regarding breaches of this fundamental right. Communication privacy may only be suspended under very strict conditions, for the institution or course of criminal proceedings or for reasons of national security when prescribed by law and on the basis of a court order.

The Constitutional Court rejected the Information Commissioner's request for formal reasoning, as the applicant did not show that the question of constitutional

review arising in connection with a procedure he was conducting and therefore procedural conditions have supposedly not been fulfilled. The Constitutional Court was of the opinion that the Security Agency Act is precise enough in defining that wiretapping of international communications (so-called strategic surveillance of international communications) is only allowed when the telephone number and person are not defined. It has to be stressed that during the inspection process the Commissioner has found out that the surveillance was conducted according to the specific telephone number and hence an identifiable person. The law, however, does not allow that for the strategic surveillance of the international communication, but the constitutional legal question of this case was whether the surveillance of the strategic international communication can be allowed by the director of the Surveillance Agency as the law stipulates or only the court has that power as Constitution demands. The question remains unanswered. The Commissioner was of the opinion that the article giving the director the power to order surveillance was unconstitutional.

C. Major specific issues

In addition to the role of the inspection supervision body and offence body, the Commissioner has conducted various other tasks with regard to the provisions of PDPA.

Since the performance of **biometric measures** is allowed only after the receipt of the Information Commissioner's decision, a total of only 16 applications were received in 2008 (compared to a total of 40 applications in 2007). Proportionally, a decrease was noted in the number of decisions issued – 17 decisions in 2008 compared with 35 decisions in 2007.

A slight increase was noted in the number of granted permits for the **connection of filing systems**. In 2008, the Information Commissioner issued a total of 8 (compared to 7 in 2007) decisions regarding the connection of filing systems.

In the framework of its **inspection activities** (as of December 2007, there have been ten state supervisors for data protection - inspectors employed with the Commissioner) in 2008 the Information Commissioner received 635 (256 in the private sector and 379 in the public sector) applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act. Compared with previous years (406 cases in 2007 and 231 in 2006) a constant and significant increase has been noted (76 % in 2007 and 56 % in 2008). As in previous years most complaints pertained to the disclosure of personal data (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 was noted in initiated administrative offence procedures: 279 cases in 2008 compared with 133 cases in 2007 and 41 cases in 2006.

In 2008, the number of requests for **written opinions** and clarifications amounted to 853. Although a slight decrease was noted compared with 1144 cases in 2007, these figures still exceeded 616 cases in 2006. This reflects a high level of public awareness of the right to privacy brought –into effect by a modern Personal Data Protection Act and is also probably related to the transparent work and intensive public campaigning performed by the Information Commissioner.

The result of this is that the Commissioner has enjoyed a good reputation, public trust and public awareness of his activities, which is reflected in findings of domestic public opinion polls, as well as from the Report on the findings of the Flash Eurobarometer survey on Data Protection from January 2008. The latter results showed that Slovenia is among the most successful EU countries in terms of citizens and data controllers' awareness about data protection and awareness about legal and institutional regulation in this area.

In December 2008, the Information Commissioner received the national Netko award for the best business and administrative website in the category of public administration institutions.

In addition to publishing non-binding opinions in the form of written explanations on his website and besides publishing a number of brochures on matters of data protection, in 2008 the Commissioner began publishing **Guidelines** on specific matters of data protection. The

purpose of the Information Commissioner's guidelines is to provide common practical instructions and information for data controllers in a form of typical frequently asked questions and answers. With the help of such answers and guidelines, data controllers should accordingly be able to comply with the statutory provisions of the Personal Data Protection Act. Last year, the Commissioner prepared and published on his website the guidelines regarding protection of personal data in hospital information systems, Guidelines regarding biometrics, Guidelines for personal data protection in employment relationships and Guidelines regarding video surveillance.

In the context of the Second European **Data Protection Day** the Commissioner organised a round table debate on safe use of the Internet and other modern technologies. The debate was centred on young technology users and personal data protection in that context. A brochure was produced aimed at informing young people, parents and teachers, published on the Commissioner's website, and distributed widely throughout all schools in Slovenia. On this occasion, the Information Commissioner also presented the awards for good practice in personal data protection in the public and private sectors.

International cooperation

The Commissioner hosted two important international meetings in 2008. In spring time he organised the **16th Case Handling Workshop** dealing with issues of biometrics in the public and private sectors, and data protection on the Internet. The event took place in Ljubljana. In September 2008, the Commissioner also hosted the **Third European Conference of Information Commissioners** where attention was drawn to a more effective and, above all, rapid implementation of the right to access public information.

In the framework of the **Schengen evaluation of Switzerland** to enter the Schengen area, the Slovenian Information Commissioner led the team of EU experts in the area of data protection. The evaluation was concluded successfully with a final report in the autumn.

The representatives of the Commissioner actively participated in a number of **international meetings and events**, among others, at the spring conference of European supervisory bodies for data protection in Rome (April) and at the 30th international conference of the data protection commissioners - "Protecting privacy in a borderless world" in Strasbourg (October), at the Central and Eastern European Data Protection Authorities forum in Poland, at the International Working Group on Data Protection in Telecommunications meetings, and many others.

The representatives of the Information Commissioner have regularly participated in the following **EU bodies** dealing with personal data protection: Working Party 29, Joint Supervision Body of Europol, Joint Supervision Authority of Schengen, Customs Joint Supervision Authority and Eurodac Supervision by EDPS - DPAs Coordination. Regular cooperation with the **Council of Europe** took place foremost in the framework of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data.

Spain

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

Due to the General Elections held in Spain last year (both Legislative chambers were dissolved and re-elected after the elections), the Parliament did not pass any piece of legislation concerning data protection implementing the Directive 95/46/EC or in the Telecommunication sector.

B. Major case law

National Court

During 2008, the National Court rejected a total of 166 appeals against resolutions by the Agency, which were fully confirmed (72 %). Of those judgments, 76 referred to claims for cancellation of data in the Baptism Books. 14 judgments partially admitted the appeals (6 %). 48 judgments fully admitted the claims to cancel resolutions by the Agency (21 %), 22 being those concerning the Baptism Books handed down after the Supreme Court Judgment of 19 September 2008 as explained later on. On one occasion, the National Court did not admit an appeal to proceedings. We can highlight the following interesting rulings:

- The ruling of 17 December 2008 finds that the mere indication of the time-off work is not health data and does not involve the deployment of high level security measures.
- The ruling of 10 July 2008 clarifies the concept of publicly available sources, considering that the Internet as a whole cannot be considered "mass media".
- The rulings of 26 February and 23 July, for public or private ownership of the filing systems, respectively, of professional associations and public health centres.
- Three judgments of 1 October 2008 ruling on the appeals regarding the processing of data of public people conducted by social mass media.

Supreme Court

For its part, the Supreme Court upheld all the resolutions issued by the Agency, except those concerning the Baptism Books of the Catholic Church.

The Supreme Court, by judgment of 19 September 2008, revoked the ruling of the National Court in which it reaffirmed the view held by the AEPD since 2004 regarding the consideration of the Baptism Books as filing systems, as organised sets of personal data, and the application to the Baptism Books of the principle of data quality in relation to accuracy and up-to-date data.

Based on these criteria the AEPD found that citizens' complaints should lead to a marginal annotation in the Baptism Books, reflecting the right of cancellation. Furthermore, the National Court in its first ruling, established that claims must be addressed from people exercising their freedom of conscience, when they feel troubled by the contents of the Baptism Book and want to register their opposition to being considered as a member of the Catholic Church.

The Supreme Court nevertheless concluded that the baptism books cannot be considered as filing systems as quoted above, "*Baptism Books are a mere accumulation of data that supposes a difficult search, access and identification because they are not classified alphabetically or by date of birth, but only for the dates of baptism*".

The AEPD presented an application before the Constitutional Court, together with the Attorney General of the State, considering that the interpretation of the term "filing system" may unduly restrict the scope of data protection rules and ignores the scope of the fundamental right recognised by the Constitutional Court's jurisprudence.

It declared in 9 judgments that the appeals filed against judgments by the National Court that confirmed the resolutions by the Agency, concerning the right to cancellation from the Baptism Books of the Catholic Church, were appropriate.

It declared the appeal filed against judgments that confirmed the resolutions by the Agency to be inappropriate on 8 occasions.

On one occasion it refused to admit an appeal filed against judgments that confirmed the resolutions by the Agency.

Resolutions by the Spanish DPA

The greater visibility that the AEPD has among the citizens has led to a sharp increase in reported offences. In that sense, the inspection actions prior to the start of sanction procedures increased 45.4 % and the procedural resolutions started nearly doubled (with an increase of 94.1 %). The sectors in which most inspections were performed continue to be those of telecommunications, financial institutions and video surveillance, overall amounting to 50.9 % of all those carried out.

In the case of the resolutions for penalisation proceedings against private companies, the top two places were also occupied by the telecommunications sectors and financial institutions, although with much higher growth than the previous year (81.3 % compared with 45 % and 58.8 % against 104 %, respectively). However, the sector where the greatest increase in penalisation procedures has taken place is that of video surveillance (which has experienced an increase of 633.3 %), although these ended in an established offence in 61.3 % of the cases. The resolutions declaring breach of the LOPD by the Public Administrations grew by 19.7 %. Likewise, resolutions terminating the procedure increased (113 %) as well as reports not admitted (138.3 %). With regard to the penalisations declared, there was an increase in penalties for severe offences (551 compared with 350). The number of cases in which a notable decrease in liability of offenders was noted came to 229, that is 42 % of the total resolutions imposing a fine (against 32 % in 2007). With regard to the concerns that most affect the citizens, it is worth noting the receipt of cold calls by citizens. As explained later on, as a result of this, the AEPD conducted two *ex officio* sectorial inspections on telephone calls and text messages to mobile telephones and it noted deficiencies in the mechanisms available to citizens to oppose receipt of such calls and warned of the risks associated with hiring additional tariff services (SMS Premium).

It is worth highlighting two interesting resolutions.

- In resolution 00281/2007 the AEPD fined two companies for obtaining personal data from a minor without the consent of their parents through a form on a website and the use of these data to send advertising materials for a credit card, without the child's legal representative's consent.

  The company did not act with due diligence to prevent processing taking into account the date of birth of the child. The AEPD declared to the entity two infringements of the Data Protection Act. The first was a serious infringement for collecting data of the minor without the consent of parents or guardian, and a very serious infringement for communicating personal data of the child to a second entity to conduct an advertising campaign. On the other hand, the Agency declared a serious infringement upon the second company acting as a data controller for using the data without their consent in the advertising campaign conducted at its instruction.

  For the AEPD, and according to applicable regulations, minors under the age of fourteen years, who are not mature enough to guarantee full understanding to give consent, it is necessary that consent be obtained from their parents or guardians, and must provide appropriate information to this end, verifying the child's age and, if in doubt, refrain from processing their data.

- In resolution AP/00061/2007, the AEPD declared a very serious breach of the LOPD for the infringement by a Public Administration of the duty of secrecy, for the publication in an Official Journal of a resolution publishing data on the beneficiaries of grants to help the treatment of drug addiction including first names, surnames and identity card numbers. The AEPD believes that to comply with the statutory requirement of "transparency, objectivity and concurrence" it was not necessary to identify the beneficiaries of aid for the treatment of drug addiction. In fact, there are alternatives, such as anonymisation or dissociation as not to identify those involved. For the AEPD, although the publication of data in official gazettes is allowed under the law, it is necessary to revise the criteria for the incorporation of data into the publications by public bodies and institutions.

C. Major specific issues

During 2008, the AEPD focused their efforts on the following issues.

More facilities to fulfil the law
One of the most effective means to protect citizens is to ensure that those using their data know how to process them; that is, to facilitate fulfilment of the law by increasing efforts to bring knowledge of it to the public and provide answers to any doubts that might arise. Traditionally, the Citizens' Enquiries Department and queries to the Legal Office were the channels to deal with that requirement.

However, 2008 was a turning point in that sense, due to a determined policy aimed at increasing the offer of information, through instruments such as publishing guides to spread the basic aspects of data protection, in a clear, simple, understandable language. That was the aim behind publishing the "*Data Protection Guide for controllers*" and the "*Data security guide*", in response to the increased demand for information on that subject. Moreover, as implementing regulation of the LOPD increased the requirements for the Agency to know the criteria applicable to it, the "*AEPD Open Sessions*" were set up and were successful in terms of attendance (2,000 people) and participation.

These incentives have complemented the traditional prevention policies based on *ex officio* sectorial inspections, such as those performed in 2008 on "commercial telephone calls and on mobile telephony text messages". The inspections were accompanied by drafting of reports or declarations on new challenges in matters of data protection, especially with regard to Internet services.

These guides can be found at the following links:
"Data Protection Guide for controllers"
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf
"Data Security Guide"
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

Information as a key element in citizens' awareness
The AEPD has the priority objectives of ensuring that citizens know the rights to which they are entitled, informing them on how to exercise those rights and putting in place instruments of prevention and coercion to guarantee their effectiveness.

The first of these demands is associated with encouraging and ensuring that the media play an active role in the dissemination of the effect personal data protection has on the daily lives of citizens and especially in the new realities related to the information society services. The bid the AEPD has made to strengthen communication by the Agency has amounted to an increase in quality. The increased presence of the Agency and personal data protection in the media has become a reality: the number of interviews and requests for information doubled in 2008, with more than 800 requests.

From a quantitative point of view, in 2008 the Legal Office answered a total of 690 queries (25 % more) of which 279 (40 %) were made by the Public Administrations and 411 (60 %) by the private sector. With regard to filing system registration, 250,000 were registered at the General Data Protection Registry (RGPD), reaching a figure of 1,267,579 (85,083 publicly held and 1,182,496 privately held), with an increase of 31 % on the previous year.

There has also been highly significant growth in the publicly held filing systems registered at the RGPD, by more than 23,500 (a 300 % increase). At this point, it has to be emphasised that the registration by the General Council of the Judicial Power of all filing systems linked to the judicial bodies (11,965). This has been an initiative that must be valued as a solid basis to encourage adaptation of the LOPD to the Judicial Administration.

Special attention to minors
Protection of the personal data of minors has become consolidated as one of the matters that the AEPD has paid preferential attention to. Various efforts have been made to encourage social awareness of these issues, such as the "Guide on the rights of boys and girls and the duties of mothers and fathers", a document with basic recommendations to provide awareness of data protection within the setting of family and school, presented on the occasion of the Internet Day held on 17 May.

The Agency also declared, when participating in the 30th International Data Protection Authorities Conference, that training in the basic use of computer tools, with their risks and advantages, is insufficient. In any case, an urgent challenge must be undertaken: to develop effective tools to know whether the users of Internet services are minors, for which help from their parents must be obtained.

In that sense, the AEPD has settled a first case of illicit processing of the data of a minor without prior verification of his age, which led to a fine being imposed due to lack of diligence in age checking.

The link to the "*Guide on the rights of boys and girls and the duties of mothers and fathers*" can be found at; https://www.agpd.es/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf

Internet vs. Privacy

The Web 2.0 has multiplied the offer of new services that are being received by Internet users on a massive scale, as it allows them to interact with each other.

One must mention social networks, powerful channels for communication and interaction that bring together large numbers of young users, including minors which, however, may generate risks to personal data protection. Being aware of this, the AEPD began an analysis of the implications of social networks in 2008 and, on initial evaluation, the following is apparent:

- Information on privacy policy and terms of use is not very clear and accessible;
- Absence of applications to check the age of minors who attempt to access the service.;
- The possibility of third parties, other than the persons classified as "friends" or "direct contacts" by the users, to access their profiles.

An urgent mission: towards international privacy standards

The diversity of data and privacy protection systems, or lack thereof, led to different problems which may be solved through the adoption of (minimum) international standards to provide guarantees to data flows in a globalised world.

The AEPD considered that the time had come to implement initiatives to allow tangible progress to be made in achieving those international standards. To that end, at the 30th International Data and Privacy Protection Conference, a joint Proposal was presented to the Swiss Authority concerning the urgent need to protect privacy in a world without frontiers. A proposal was made to the Authority organising the International Conference in 2009 to create and coordinate a working party that would have the objective of preparing and submitting a "*Joint Proposal to Draft International Standards for Protection of Privacy and Personal Data*" to the Closed Session of the 31st Conference.

The Proposal was unanimously approved by the Conference, thus leaving the AEPD in charge of the process of forming the Working Group and leading the project to develop the proposal of international standards for the protection of privacy with regard to the processing of personal data. The ultimate purpose would be that the text presented to the Conference in November in Madrid could be adopted by wide consensus and act as a basis to become an international instrument for protection of privacy and personal data.

Cooperation with the data protection agencies of the autonomous communities

In matters of inspection, cooperation between the Data Protection Agencies has advanced and is being improved in the analysis of the measures that allow one to guarantee the effectiveness of the resolutions passed and coordination of the inspection actions when the investigations affect the competencies of several Agencies. Likewise, criteria have been exchanged concerning matters of video surveillance, judgments published on the web and publication of personal information in Official Journals and Gazettes. The Agencies have shared the priority objective of the need to encourage education of minors and they have backed the candidacy of the AEPD to organise the 31st International Data Protection and Privacy Conference. This backing is accompanied by a commitment to collaborate in performing work to prepare a document of common standards of data protection in a globalised world.

Enforcement: enhancement of preventive actions

Ex officio sector plan on telephone advertising

The AEPD has conducted an *ex officio* sector plan on telephone advertising in which it has analysed the practices of the major mobile and fixed telephony operators in Spain and of entities providing additional rate (Premium) services based on the receipt of SMS messages or subscriber services.

As a general finding, the AEPD has detected deficiencies in the guarantee systems for citizens to avoid telephone advertising. Among the major conclusions of the analysis carried out, the AEPD has stressed the deficiencies in the mechanisms available to citizens so that they may prevent, in some cases, and object to the receipt of commercial communications via messages and calls to fixed and mobile telephone numbers, and it has warned of the risks associated to the contracting of additional rate services. According to the report, the major deficiencies detected in the inspection are the following:

- According to the data from the sector plan, 53 % of the companies analysed consult telephone directories to select the recipients of their campaigns via calls to fixed telephone numbers. In this respect, attention has been drawn to the fact that only 1 % of the subscribers listed in telephone directories has requested not to receive commercial calls.
- Some practices declared by operators, such as the use of data on 'recommended individuals' have already been sanctioned by the AEPD.
- It has been found that random calls without identifying the holder of the number represent a usual method for mobile telephone campaigns. The AEPD considers it urgent to establish a legal framework to prohibit this practice.
- Senders of messages are required to provide clear information, as well as simple methods for exercising the right to object to their receipt.
- Operators should establish control mechanisms to limit the massive influx of unsolicited commercial text messages from countries outside Europe that do not comply with Spanish regulations.
- Regarding premium services, the *ex officio* sector plan stresses that the information clauses included in the advertising of these services contain very little information, because usually incomplete or abbreviated words are used in messages to mobile phone numbers and they provide information sign that are difficult to read. Therefore, they are not informed of the cost of the messages, the procedure for unsubscribing, and the data that will be processed, etc. With respect to these services, the AEPD issues a special warning on the contracting of these services by minors, one of the most vulnerable sectors, because they are more susceptible to deception than adults.

After carrying out the sector plan and as a result of the deficiencies that were found, the AEPD prepared a number of **recommendations for citizens enabling them to enforce their rights, and for the sector,** so that they may improve its practices.

The full *ex officio* plan and the recommendations are available through this link:
https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/plan_sectorial_publicidad_telefonica_2008.pdf
https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_sms_llamadas_11_2008.pdf

Video surveillance

In 2008, the AEPD began an *ex officio* investigation on different websites that disseminated images in real time taken by security cameras installed in public areas in order to clarify whether the password needed to grant access to these images was correctly installed or there was a lack of security measures put in place as required in the data protection regulations.

Codes of Conduct

Self-regulation, through standard Codes notified and registered with the Registration Department, is a complementary instrument to facilitate fulfilment of the LOPD and increase legal security. Throughout 2008, self-regulation initiatives were set up in the private insurance mediation sector, employers' mutual insurance for occupational illness and accidents in the workplace, clinical research and pharmaceutical surveillance, security companies and law firms.

Main Developments in Third Countries

Spain's activities in the Ibero-American Data Protection Network

The need to respond to new international challenges has required a qualitative change in the activity of the Ibero-American Network for Data Protection, whose guidelines are:

- To strengthen the institutional representation of the participating countries and strengthen their effectiveness.
- To promote the executive organisation of representatives from Latin American countries.
- To open up participation in the meetings of the network to third countries not belonging to the Ibero-American environment.
- To promote an exchange of views between political institutions and private companies.
- To provide a flexible dialogue between Latin American countries and the European Commission on efforts to obtain Declaration of Adequate countries in guarantee of personal data protection.
- To incorporate the Ibero-American Network into the process of formulation of international data protection standards.

The VI Ibero-American Meeting on Data Protection, held in Cartagena de Indias (Colombia) from 27 to 30 May 2008 has laid the foundation for achieving these objectives. Institutions involved were representing Latin American countries as well as U.S. authorities in North America, and speakers from foreign multinational corporations.

A Network regulation was updated whereby the AEPD shall assume the duties of Secretary and hold the Presidency for a period of two years along with four members with specific roles assumed by Argentina, Chile, Mexico and Portugal. As of March 2009, the Ibero-American Network will participate as an observer in the biannual meetings of the Consultative Committee of Convention 108 of the Council of Europe.

The Agency has continued to develop bilateral cooperation, which culminated in the signing of the Letter of Intent for Mutual Cooperation between the International Agency for the Development of the Information Society in Bolivia (ADSIB) and the AEPD and the "Memorandum of Understanding between the Corporation for the Promotion of Production of Chile (CORFO) and the AEPD.

Sweden

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

Directive 95/46/EC is transposed into Swedish law as the *Personal Data Act* – PDA - (1998:204) which came into effect on 24 October 1998. The PDA is supplemented by the *Personal Data Ordinance* which came into effect the same day. The Act applies, like 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 personal 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.

Directive 2002/58/EC is transposed into Swedish law as the *Electronic Communications Act* – ECA – (2003:389) which came into effect on 25 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 is supervised by the National Post and Telecom Agency. Article 13 of the EC Directive regarding unsolicited e-mail is transposed into Swedish law as amendments to the *Marketing Practices Act* (1995:450). The amendments came into effect on 1 April 2004. The Marketing Practices Act falls under the supervision of the Consumer Agency.

In 2004, the Government decided to set up a Committee (Integritetsskyddskommittén – Committee on the protection of privacy) composed of members of the Riksdag (the Swedish Parliament) and experts with the task of carrying out a survey and analysis of the legislation in Sweden concerning privacy. The Committee was later assigned the task of considering if, in addition to the existing legislation, there was a need for generally applicable rules to protect privacy. As was informed in last year's Annual Report, the Committee presented an extensive report in spring 2007 containing a survey and analysis. The Committee also expressed several points of criticism of a systematic and methodical nature and gave a negative answer to the direct question whether the protection of privacy could be considered as satisfactorily regulated. In January 2008, the second and last report of the Committee was presented and in this report the Committee gave an analysis on how the constitutional protection of privacy ought to be regulated and what other measures are necessary. One of the proposals of the Committee was that the constitutional protection of privacy be strengthened. In this respect the Committee proposes protection against public authorities' surveillance and mapping-out of the individual's personal circumstances. The Committee mentions, among other things, secret surveillance and retention of traffic data as examples of infringements where there ought to be a more thorough examination than is the case today.

As was reported last year the *EC Directive on the retention of data processed in connection with the provision of public electronic communication services* had not yet been transposed into Swedish law and it still has not. The Government will probably submit a Bill to the Riksdag in June this year.

In July 2008, a new Act on patient records and healthcare, the *Patient Data Act*, came into effect. The Act can be described as a cohesive regulation of personal data within health and medical services.

In June 2008, the Riksdag approved the Government's proposal for a new *Signal Surveillance Act* in defence intelligence activities. The Act applies to all signal surveillance for defence intelligence purposes – whether transmitted over the air or by wire. The Act contains a number of rules designed to protect the individual's privacy. However, the Riksdag requires further control mechanisms to, among other things, increase the protection of individuals. The Data Inspection Board will be specially commissioned to follow the activities of the National Defence Radio Establishment and shall report back to the Government by December 2010. The new legislation came into effect on 1 January 2009.

The third *EC Directive on money laundering* was transposed into Swedish law in 2008 and the new legislation came into effect on 15 March 2009.

In December 2008 the Government submitted a proposal for a new Act transposing the *Intellectual Property Rights Enforcement Directive* (2004/48/EC) into Swedish law. The Riksdag approved the proposal and the Act will come into effect on 1 April 2009. One specific feature of the Act is that organisations protecting intellectual property- if they suspect that someone has been involved in illegal peer-to-peer file sharing - may turn to a court of law and require that Internet providers disclose information about the IP address owner in question.

In December 2006, a Commission of inquiry was set up and was assigned the task of abolishing the monopoly of Apoteket AB (National Cooperation of Swedish Pharmacies) to sell pharmaceuticals and make it possible for other operators to sell such products. The assignment also included issues regarding for instance registration of prescriptions. The Data Inspection Board was consulted and gave its opinion especially as regards database issues. The Government recently submitted a Bill to the Riksdag with a proposal for a new Act, the *Act on Pharmacy Data*. The new Act is proposed to come into effect in July 2009.

In September 2008, the Data Inspection Board gave its opinion on proposals for amendments to the *Credit Information Act* implying that in practice there will be the same requirements on credit information on the Internet as on other forms of credit information activities. The background for the proposals was an amendment to the *Fundamental Law on Expression* (a constitutional law) in 2003, which led to the possibility to disclose credit information on websites to anyone without having to comply with the strict rules of the *Credit Information Act*. This has lead to infringements of privacy and many complaints.

In February 2008, the Government set up a Commission of inquiry with the task of reviewing legislation on video surveillance. The assignment includes carrying out a survey and analysis of the application of the current legislation. The inquiry shall, among other things, consider whether there is need for further measures in order to strengthen the protection for the individual's privacy in connection with video surveillance.

B. Major case law

The Data Inspection Board has in two previous Annual Reports presented cases concerning biometric data in schools. Students' fingerprints were taken and processed in an automatic plate machine for the purpose of checking access to the school canteen. In December 2008, the Supreme Administrative Court decided that schools may use the students' fingerprints to check whether they have paid for the meal or not. However, the students must give their consent and there must be an alternative for those who do not wish to use their fingerprints.

In a decision of 2007, the Data Inspection Board ruled that the Swedish Builders Workers' Union had to stop processing data regarding wages for those workers who were not members of the union. An appeal was lodged against the decision before the County Administrative Court which in December 2008 turned down the appeal and upheld the Data Inspection Board's decision. The Builders Workers' Union has appealed to the Administrative Court of Appeal where the case is now pending.

The Data Inspection Board has during 2006 – 2008 carried out inspections regarding public transport companies' new ticket systems with smart cards that leave electronic traces (systems based on RFID-techniques). When the passenger uses his electronic ticket the following data is recorded: card number, date, time and stop/gate. If the card holder has registered his smart card with the transport company the card number is connected with the passenger's personal identification number, name and address. In this way, the electronic traces from the card can be connected to a certain person. The Data Inspection Board decided that such traces could only be stored for 60 days and thereafter be unidentified. One of the transport companies concerned appealed against the Data Inspection Board's decision to the County Administrative Court which in January 2009 repealed the Board's decision and remitted the case for a new review.

During 2007, the Data Inspection Board inspected how housing firms and housing cooperatives processed personal data in electronic key systems. The electronic

key belongs to a certain flat and often leaves data in a passage log regarding when and where the resident has used the key. The inspection showed that personal data was not processed in a proper way. The Data Inspection Board issued guidelines on how to use electronic keys in housing firms and housing cooperatives. The Board has a very restrictive view as to the use of data for other purposes than to open doors or book a laundry time. In July 2008 the Board decided in a case regarding a housing firm where, among other things, the data from the electronic key was used to see who had used the laundry room. The Board ordered the housing firm to stop using the passage logs for this purpose. An appeal was lodged against the decision before the County Administrative Court which upheld the Data Inspection Board's decision. The housing firm has now, in 2009, appealed to the Administrative Court of Appeal.

In 2008, the Data Inspection Board sent out a web questionnaire to schools and one of the issues was if and to what extent schools used video surveillance on its premises. The result showed that video surveillance had increased by 150 % compared to 2005 when a similar investigation was made. The Data Inspection Board then inspected seven schools and found that the video surveillance of students during daytime in many respects infringed against the Personal Data Act. The inspections also showed that there was a considerable lack of knowledge of the legislation on data protection and the Board therefore issued a checklist to make it easier for the schools to decide when video surveillance is permitted. Appeals were lodged against the Board's decisions of 1 October 2008 before the County Administrative Court where they are now pending.

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 have been published during 2008.

As was reported last year, the Data Inspection Board has been assigned by the Government the task of contributing to a secure and efficient eGovernment. The Board earlier issued guidelines for the municipalities and in 2008 two sets of guidelines were drawn up; one for Government authorities, *eGovernment and the Personal Data Act,* and one for all public authorities, *IT-security and public authorities' e-services*.

We also produced a report *Privacy Year 2008,* a comprehensive survey of new legislation, proposals, decisions and techniques that affected privacy during the year.

A second report concerning the attitude of young people, especially towards the Internet, was published during 2008 and the report *Young People and Privacy* was also presented at the 30th International Conference on data protection held in Strasbourg.

Sector agreements

During 2008, at the initiative of Data Inspection Board, the property sector, set out to draw up a sector agreement (Code of Conduct) aimed at regulating the use of video surveillance in apartment blocks. This initiative was taken up due to the rise in complaints regarding such video surveillance. The sector agreement will probably be completed in June 2009.

The Nordic Case Handling Workshop

The Data Inspection Board in May 2008 hosted the annual *Nordic Case Handling Workshop* with participants from Denmark, the Faeroe Islands, Finland, Iceland, Norway and Sweden.

The United Kingdom

A. Implementation of Directive 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 Data Protection Act 1998.

B. Major case law

A judgement in 2008 by the European Court of Human Rights in the case of S. and Marper v. the United Kingdom ruled that the "blanket and indiscriminate" retention of DNA cellular samples and profiles of persons suspected but not convicted of offences was disproportionate and failed to strike a fair balance between the rights of the individual and the interests of the state.

Following this judgement the UK government committed to publishing a White Paper on the collection and use of forensic information in 2009.

The Marper judgement is of considerable significance for the ICO and will have implications well beyond the retention of DNA and fingerprints as it provides authoritative support for the approach we have taken to several aspects of the privacy of personal information.

The ICO now has observer status at all meetings of the National DNA Database Strategy Board.

C. Major specific issues

We marked European Data Protection Day in January by launching our revised CCTV code of practice at the Houses of Parliament.

We took enforcement action against several organisations, including Carphone Warehouse (CPW) and Marks & Spencer (M&S). The investigation into CPW followed complaints concerning the way personal information was stored and processed; and the action against M&S was taken after an unencrypted laptop containing 26,000 employees' details was stolen.

We prosecuted 17 organisations, including a Manchester debt recovery company for bombarding individuals and businesses with unwanted faxes; and a solicitor and accountant for failing to notify as data controllers.

On 25 June, four reports were published on the handling of personal information. The ICO published its response to these reviews in November.

The Data Handling Review
A review of data handling procedures in government, set up by the prime minister in response to the loss of over 25 million citizens' personal details by Her Majesty's Revenue and Customs (HMRC) in 2007. The review was led by Sir Gus O'Donnell of the Cabinet Office. One of its recommendations was that was that privacy impact assessments should be used by all central government departments.

The review of information security at HMRC
The Chancellor of the Exchequer commissioned Kieran Poynter, the Chairman of PricewaterhouseCoopers, to conduct an investigation into the loss of personal data at HMRC, as well as conducting a root and branch review of processes and systems as they relate to data handling at HMRC.

The Independent Police Complaints Commission (IPCC) independent investigation report into the loss of data relating to Child Benefit.
The IPCC, having jurisdiction by virtue of the Police Act 2002, initiated its own investigation into the series of events leading up to the loss of data at HMRC in order to ascertain whether any criminal conduct or disciplinary offences had been committed by HMRC staff.

The report into the loss of Ministry of Defence (MOD) personal data

On 9 January 2008, a Royal Navy laptop computer containing unencrypted records for more than 600,000 people was stolen. The Secretary of State for Defence commissioned Sir Edmund Burton to conduct a review to establish the exact circumstances and events that led to the loss by MOD of personal data; to examine the adequacy of the steps taken to prevent any recurrence, and of MOD policy, practice and management arrangements in respect of the protection of personal data more generally.

The Data Sharing Review, carried out by Richard Thomas and Dr Mark Walport, on behalf of the Prime Minister, was published on 11 July. The report made a series of recommendations aimed at transforming the personal and organisational culture of those who collect, manage and share information. We submitted a response to the review consultation.

We launched our data protection strategy at our data protection officers' conference in Manchester in March and we launched our privacy by design report at our conference in Manchester in November. The privacy by design report urges organisations to take simple steps to improve organisational and technological measures to better protect personal information and is intended to help organisations adopt new privacy by design techniques. It highlights the need to make sure privacy is considered properly by organisations and from the start when they are developing new information systems.

During 2008, the Commissioner provided responses to 47 consultations (this is the same number as in 2007).

During 2008, the Commissioner provided evidence to the following Parliamentary committees.

- House of Commons Home Affairs Committee: 'A Surveillance Society?' report.
- House of Commons Home Affairs Committee: inquiry into 'The Surveillance Society'.
- House of Lords select committee on the Constitution: inquiry on 'The impact of surveillance and data collection upon the privacy of citizens and their relationship with the State'.
- House of Lords Select committee on the European Union, Home Affairs sub committee: inquiry into the Framework Decision on Passenger Name Records.
- House of Lords Select Committee on the European Union: Inquiry into Europol.
- House of Lords Science and Technology Committee: Genomic medicine - implications of the generation and storage of genome data on personal data security and privacy.
- House of Commons Public Bill Committee: committee stage of the passage of the Counter-Terrorism Bill.

The ICO also submitted written evidence to the Thomas/Walport review of information sharing and met with the review team.

By the end of 2008 we had received 340 notifications of security breaches and we had developed guidance for organisations on how to deal with security breaches involving personal data.

Chapter Three
European Union and Community Activities

3.1. EUROPEAN COMMISSION

Commission Decision 2008/49/EC of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data[25]

The Commission decided to complement the Decision by setting up IMI with regard to the personal data protection provisions. Since the various tasks and functions of the Commission and the Member States in relation to IMI will entail different responsibilities and obligations as regards data protection rules, this Decision defines their respective functions, responsibilities and access rights, as suggested in the opinion of the Article 29 Working Party on data protection issues related to the Internal Market Information System (IMI)[26].

Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems[27]

This Recommendation to the Member States provides a set of guidelines for developing and deploying interoperable electronic health record systems, allowing for cross-border exchange of patient data within the Community as far as necessary for a legitimate medical or healthcare purpose. Such electronic health record systems should enable healthcare providers to ensure that a patient receives care more effectively and efficiently by having timely and secure access to basic and possibly vital, health information, and if so needed and in conformity with the patient's fundamental rights to privacy and data protection.

3.2. EUROPEAN COURT OF JUSTICE

Judgment of the Court (Grand Chamber) of 29 January 2008 — Productores de Música de España (Promusicae) v Telefónica de España SAU (Case C-275/06)[28]

Operative part of the judgment:

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, Community law requires that, when transposing those directives, the Member States take care to interpret them in a way that allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not interpret them in a way that would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

Judgment of the Court (Grand Chamber) of 16 December 2008 – Heinz Huber v Bundesrepublik Deutschland (Case C-524/06)[29]

Operative part of the judgment:

1. A system for processing personal data relating to Union citizens who are not nationals of the Member State concerned, such as that put in place by the Law on the central register of foreign nationals (Gesetz über

[25] OJ L 013 , 16/1/2008 p. 18 – 23.

[26] Opinion 01911/7/EN, WP 140.

[27] OJ L 190, 18.7.2008, p. 37–43.

[28] OJ C 64 of 8.3.2008, p .9.

[29] OJ C 44 of 21.2.2009, p. 5.

das Ausländerzentralregister) of 2 September 1994, as amended by the Law of 21 June 2005, and having as its object the provision of support to the national authorities responsible for the application of the law relating to the right of residence does not satisfy the requirement of necessity laid down by Article 7(e), Directive 95/46/EC of the European Parliament and of the Council 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, interpreted in the light of the prohibition on any discrimination on grounds of nationality, unless:

- it contains only the data which are necessary for the application by those authorities of that legislation, and
- its centralised nature enables the legislation relating to the right of residence to be more effectively applied as regards EU citizens who are not nationals of that Member State.

It is for the national court to ascertain whether those conditions are satisfied in the main proceedings.

The storage and processing of personal data containing individualised personal information in a register such as the Central Register of Foreign Nationals for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of Article 7(e) of Directive 95/46.

2. Article 12(1) EC must be interpreted as meaning that it precludes the implementation by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to EU citizens who are not nationals of that Member State.

Judgment of the Court of First Instance of 8 November 2007 - Bavarian Lager v Commission (Case T-194/04)[30]

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.

[30] OJ C 315 of 22.12.2007, p.33.

3.3. EUROPEAN DATA PROTECTION SUPERVISOR

Introduction

The mission of the European Data Protection Supervisor (EDPS) is to ensure that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data, are respected by the Community institutions and bodies.

The main activities of the EDPS, as laid down in Regulation (EC) No 45/2001[31] ("the Regulation"), are to:

- monitor and ensure that the provisions of the Regulation are complied with when Community institutions and bodies process personal data (supervision);
- advise the Community institutions and bodies on all matters relating to the processing of personal data. This includes consultation on proposals for legislation and monitoring new developments that have an impact on the protection of personal data (consultation);
- cooperate with national supervisory authorities and supervisory bodies in the "third pillar" of the EU with a view to improving consistency in the protection of personal data (cooperation).

Supervision

The supervisory tasks range from providing advice and assisting data protection officers, through prior checking of risky data processing operations, to conducting inquiries, including on the spot inspections, and handling complaints.

[31] 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.

Prior checking of processing operations continued to be the main aspect of supervision during 2008, with more opinions issued than in any of the preceding years. The EDPS published more than 100 prior-check opinions, mainly covering the following issues: processing of health-related data, recruitment of staff and selection of candidates, staff evaluation, journalist accreditation, identity management systems, access control and security investigations.

While most institutions and bodies are making good progress in developing compliance with data protection rules and principles, the emphasis of supervision is shifting to monitoring the implementation of recommendations in prior checking and to improving the level of compliance in agencies. In this context, the EDPS has further developed his **inspection policy** and has completed a first series of on the spot inspections in different institutions and bodies to measure compliance in practice.

The total number of **complaints** continued to increase in 2008, with fewer admissible complaints than before, but more complexity on the whole. Admissible cases related in particular to issues such as access to data, processing of sensitive data, right of rectification and obligation to provide information.

Further work was also done in consultation about **administrative measures** envisaged by Community institutions and bodies in relation to the processing of personal data. A variety of challenging issues was raised, including transfers of medical files to national tribunals, access to public documents containing personal data, implementing rules of Regulation (EC) No 45/2001 and complaints handled by the European Ombudsman.

The EDPS continued to work on his **video-surveillance guidelines** to provide practical guidance to Community institutions and bodies on compliance with data protection rules when using video-surveillance systems.

Consultation

The EDPS has further improved his consultation role and submitted opinions on an increasing number of proposals for legislation. He has widened the scope of his interventions to a greater variety of policy areas, and to all stages of the legislative procedure.

The EDPS issued 14 opinions on proposed EU legislation and initiatives in 2008. The majority of them continued to concern issues related to the area of **freedom, security and justice**. An important development in this area was the adoption of the **Data Protection Framework Decision** in the field of police and judicial cooperation in criminal matters. Throughout the negotiations, this piece of legislation has been a major focus of attention for the EDPS who issued three opinions as well as comments on the subject.

The proposal to modify the Regulation on **public access to documents** held by EU institutions as well as the review of the Directive on privacy and electronic communications **(ePrivacy Directive)** were also given special attention by the EDPS. Matters related to **Passenger Name Records** (PNR) were also quite prominent in the EDPS's consultative activities, in particular with regard to the follow up of the EU PNR proposal.

The issue of **exchange of information** was a key focus area for the EDPS. He adopted opinions on information exchange systems that were proposed in the framework of the Internal Market Information System (IMI), Eurojust, road safety, the protection of children using the Internet, the European Criminal Records Information System (ECRIS), the EU-US High Level Contact Group on information sharing, and the European e-Justice strategy. Preliminary comments were also issued on the Commission's EU border management package. The EDPS's opinions emphasised the need for such exchange of information to be carefully assessed and to be coupled with specific data protection safeguards.

The use of **new technologies** was also addressed on several occasions (e.g. ECRIS and the European e-Justice strategy). The EDPS repeatedly called for data protection issues to be taken into account at the earliest possible stage ("privacy-by-design"). He also highlighted that technology tools should be used not only to ensure the exchange of information, but also to enhance the rights of the persons concerned.

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

A number of perspectives for future changes, which will serve as the agenda of main **priorities** for the EDPS, have been identified. They include new **technological trends** raising critical data protection and privacy concerns, such as the development of cloud computing systems[32] and DNA-sequencing technologies.

As regards new developments in **policy and legislation**, the main issues to which the EDPS intends to devote special attention include the following:

- reflection on further improvements of the **Data Protection Framework Decision** to increase the level of protection provided by the new instrument in the third pillar;
- **the future of the Data Protection Directive**;
- the Commission's multi-annual programme in the area of freedom, security and justice - referred to as the **"Stockholm Programme";**
- **major trends in law enforcement** and legislative activities relating to the fight against terrorism and organised crime;
- the revision of the Regulation on **public access to documents**;
- new initiatives aimed at enhancing **cross-border healthcare** in combination with the use of information technologies.

Cooperation

The main platform for cooperation between 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 of the Data Protection Directive.

The EDPS and the Working Party have cooperated to produce a good synergy on a range of subjects, but especially focusing on the implementation of the Data Protection Directive and on challenges raised by new technologies. The EDPS also strongly supported initiatives taken to facilitate international data flows.

The Working Party has adopted opinions on proposals for legislation, which in some cases had also been subject to the EDPS's opinions (e.g. review of ePrivacy Directive). While the EDPS's opinion is a compulsory feature of the EU legislative process, contributions of the Working Party are also very useful, particularly since they may contain special points for attention from a national perspective. The EDPS therefore welcomes these contributions which have been consistent with his own opinions.

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. The Eurodac Supervision Coordination Group – composed of national data protection authorities and the EDPS - met twice in 2008 and focused on the implementation of the work programme adopted by the Group in December 2007. Three topics had been selected within the work programme for closer examination and reporting, namely: information of the data subjects, children and Eurodac, and DubliNet[33]. At the same time, the framework in which the Group is operating has also attracted attention: the European Commission has undertaken a review of the Dublin and Eurodac Regulations, in the framework of the asylum measures in general.

The need for close cooperation between the EDPS and other data protection authorities in **third pillar matters** - the area of police and judicial cooperation - has become apparent in recent years through the increased number of initiatives at European and international levels aimed at collecting and sharing personal data.

The EDPS strives to ensure a high and consistent level of data protection in the works of the supervisory data

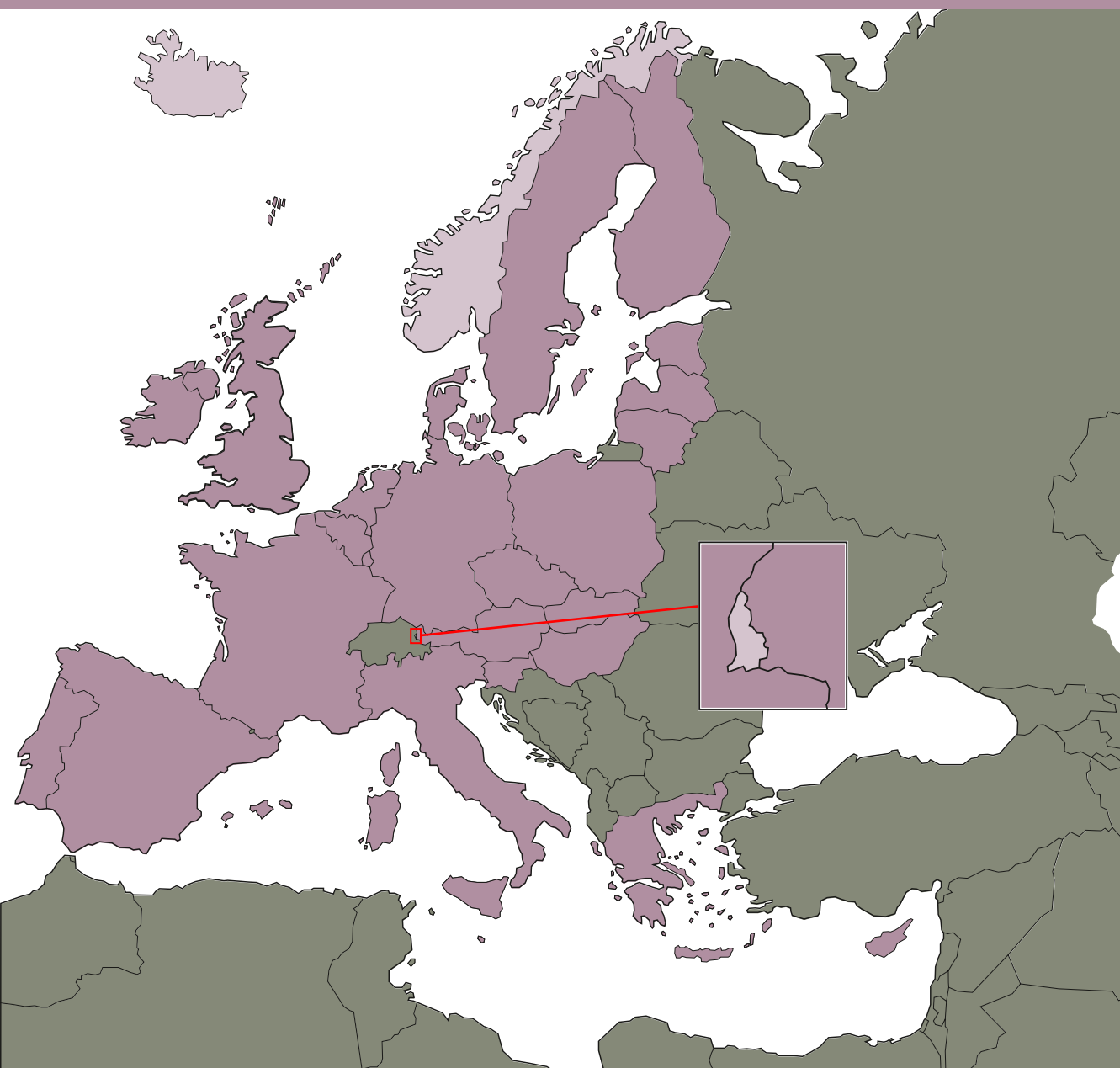
[32] Cloud computing refers to the use of Internet ("cloud") based computer technology for a variety of services. It is a style of computing in which dynamically scalable and often virtualised resources are provided as a service over the Internet.

[33] DubliNet is the secure electronic network of transmission channels between the national authorities dealing with asylum applications. Usually, a "hit" in the Eurodac system will trigger an exchange of data about the asylum seeker. This exchange will use DubliNet.

protection bodies (Joint Supervisory Bodies for Schengen, Europol, Eurojust and the Customs Information System) established under the EU third pillar. The EDPS also cooperates with national data protection authorities by actively contributing to the meetings held by the Working Party on Police and Justice.

Cooperation in other **international forums** continued to attract attention, including the International Conference of Data Protection and Privacy Commissioners organised in Strasbourg and the "London initiative" on raising awareness of data protection and making it more effective. Following similar events organised in 2005 and 2007, a third workshop on data protection in international organisations is presently under consideration.

Chapter Four
Main Developments in EEA Countries



Iceland

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

In 2008, a number of legal acts and administrative rules 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 88/2008 on Criminal Procedure. This Act contains a number of provisions affecting the privacy of individuals, most notably defendants but also, for example, witnesses. Amongst these provisions are those of Article 16 regarding access to court documents. Not only does Article 16 grant this right to the defendant and his defence council, but also to the public. Both the charge and the defendant's written account are open to the public. However, parts of these documents containing information on private, financial or business affairs shall be withheld, given that such secrecy is fair and reasonable, unless the party in question agrees to the information being given. Judgments and other court decisions shall be given to the public on demand, but in some cases, certain information must be deleted from such documents, e.g. when private interests require deletion because of special circumstances. As can be seen in Article 17, judgments and court decisions are not only to be given on demand. Courts can also publish them, e.g. on their websites, but they must pass rules on deletion of data that are not to be made public.

2. Act No 97/2008 Changing the Medicinal Products Act, No 93/1994. In 2003, new provisions were added to Act No 93/1994, cf. Act No 89/2003, on a central drug prescriptions database under the responsibility of the National Health Directorate. The provisions on this database are set out in Article 27 of Act No 93/1994. According to these provisions, the National Health Directorate has access to the database for conducting its surveillance role with regard to habit-forming or narcotic, medicinal products, its general surveillance with physicians' prescriptions, and for monitoring developments in medicinal products. The Icelandic Medicines Control Agency and the Health Insurance Institution may also be granted access when certain criteria are fulfilled. Originally, personally identifiable data were to be deleted within three years of being entered into the database. However, Act No 97/2008 prolonged this period to 30 years.

3. Act No 112/2008 on Health Insurance. In accordance with this Act, a new public institution, the Health Insurance Institution, was established. This institution has the role of negotiating with health institutions and independent health service providers on payments from public funds for health service. According to Article 46 of the Act, health professionals, who are responsible for the retention of patient files, are obliged to give the Health Insurance Institution access to the data and documents necessary for the institution to fulfil its role. However, employees of the institution may only read health files in the location where they are kept and only those parts of it that are necessary for the institution to administer health service contracts.

4. Act No 142/2008 on an Investigation of the Events Leading to, and the Causes of, the Downfall of the Icelandic Banks in 2008, and Related Events. – The Act establishes a special Investigation Commission under the auspices of the Icelandic Parliament. The Commission shall investigate the financial downturn in Iceland, which occurred in autumn 2008, and report on the conclusions of the investigation. The Commission shall, according to Article 14 of the Act, notify any suspicion of criminal conduct to the Prosecutor General. Furthermore, the Commission shall, if it considers it likely that a public servant has committed a breach of duty, notify this to the Head of Institution and to the relevant Ministry. According to Paragraph 1, Article 6, of the Act, all individuals, institutions and legal persons have a duty to provide any information, documents and explanations that the Investigation Commission may request.

Commission members and persons working on the investigation are, according to Paragraph 3, Article 4 of the Act, obliged to maintain silence as regards any confidential information received by the Commission. The Commission may however provide working groups and expert counsellors with information and documents as necessary. Furthermore, the Commission may also deliver information if necessary for mutual provisions of information and cooperation with parties abroad

engaged in investigations similar to the Commission. The party receiving information shall also be bound by a duty to maintain silence. However, according to Paragraph 4, Article 4, the aforementioned provisions shall not preclude publication by the Commission of information that the Commission deems necessary in order to provide grounds for its conclusion, even if the information would otherwise be confidential. Information on the personal affairs of individuals, including their financial affairs, shall only be published if significant public interests for disclosure outweigh the personal interests of the individual in question.

According to Paragraph 2, Article 17 of the Act, the Provisions of Articles 18–21 of the Data Protection Act, No 77/2000, i.e. the provisions on access rights and information to be provided to the data subject, shall not apply to the Commission's activities. Nevertheless, according to Paragraph 3, Article 17, persons subjected to the Commission's investigation shall, when it has completed its investigation, enjoy the rights of the aforementioned provisions of the Data Protection Act if their cases have not been made subject to criminal procedure. The right to access shall then be governed by the provisions of law on procedure in such cases.

5. Act No 160/2008 on a Service and Knowledge Centre for the Blind, Visually Impaired and Legally Blind Individuals. – According to Article 6 of the Act, the Service and Knowledge Centre shall maintain a register on all blind, visually impaired and legally blind individuals for improving the service provided to them, guaranteeing the quality of the service, supervising the provision of the service, and conducting statistical and scientific research. The processing of personal data in this regard shall be in accordance with the Data Protection Act.

6. Act No 164/2008 Changing the Act on Income Tax, No 90/2003. – Article 6 of the Act added a new provision to the Act on Income Tax, stating that banks and other financial institutions that retain deposits shall, at their own initiative, inform the National Tax Commissioner of deposit interests and money amounts on deposits at the end of each year.

7. Rules on the Obligation to Notify or Obtain a Permit for the Processing of Personal Data, No 712/2004. – These rules, passed by the DPA in accordance with the Data Protection Act, Art. 31 and 33, replace Rule No 698/2004. The most significant change is that the processing of personal data in genetic research is no longer subject to permission, given that the data subjects have consented to the processing. However, the processing must be notified to the DPA. As described in Point 8 below, the DPA has passed rules on the processing of personal data in genetic research.

8. Rule No 1100/2008 on the Processing of Personal Data in Genetic Research. – As described in Point 7 above, processing of personal data in genetic research is no longer subject to the DPA's permission if the data subject consents to the processing. The provisions of Rule No 1100/2008 must, then, always be adhered to. These provisions have taken the place of provisions relating to permissions for individual research projects. According to these rules, the data subject's consent must meet certain requirements, e.g. that he or she must be informed when data will be deleted or if they are to be retained permanently for research purposes, if it is planned to contact relatives in order to ask them to take part in the research project, and if the data subject might receive information on his or her genotype, where he or she wishes to be given such information. The rules also contain provisions on, for example, the encoding of personal data; that no one who processes genetic data may gain access to data with personal identity markers; and that those who conduct genetic research shall notify the processing of personal data in each research project to the DPA and also send a description of security measures in such research to the DPA. If the same security measures are used in more than one research projects, a common description for all these projects is sufficient.

B. Major case law

On 3 October 2008, the Supreme Court of Iceland issued a judgment regarding the National Tax Commissioner's power to demand financial data on individuals. The Commissioner had demanded data from credit card companies on all transactions on credit cards issued and charged abroad, given that the total withdrawal exceeded a certain amount. This demand was based on Article 94 of the Act on Income

Tax, No 90/2003, stating that everyone is obliged to give tax authorities the necessary information and documents that they request.

One credit card company refused to give the information demanded. In accordance with Article 94 of the aforementioned Act, the National Tax Commissioner then asked for a court decision on the company's obligation to provide the information. The District Court of Reykjavik came to the conclusion that the company was obliged to do so. The company appealed against this decision to the Supreme Court. The Court held, among other things, that the National Tax Commissioner's demand for information did not exceed the boundaries of Subparagraphs 2 and 3, Paragraph 1, Article 7 of the Data Protection Act, stating that personal data must be obtained for specified, explicit, relevant purposes and not processed further for other incompatible purposes; and that said personal data must be adequate, relevant and not excessive in relation to the purposes of the processing. Accordingly, the Supreme Court came to the conclusion that the company in question was obliged to give the information demanded by the National Tax Commissioner.

C. Major specific issues

As mentioned in the description above of legislative developments in 2008, the Medicinal Products Act No 93/1994, was changed so as to extend the retention period of personal data in a central drug prescription database from three to 30 years. This was one of the major data protection issues in 2008. The DPA issued an opinion on the parliamentary bill, in which this change to the Act was proposed, stating that this extension of the retention period was disproportionate.

Another major issue was the passing of the DPA's Rule No 1100/2008 on the Processing of Personal Data in Genetic Research, cf. the discussion on those rules in the description of legislative developments in 2008.

On 6 October 2008, the DPA issued an opinion to the Confederation of Icelandic Employers on whether it was legal for businesses to process personal data in relation to a civil recovery scheme. According to this scheme, an individual who was suspected of theft or attempted theft of goods would not be charged by the police if he or she paid a certain amount to the business in question. The individual would sign an agreement to this effect consenting to their personal data being entered into a database kept by a certain security company.

The DPA considered that it was uncertain whether agreements with individuals with regard to this civil recovery scheme would be legal. Furthermore, this would entail that private businesses would step into the role of the state, i.e. deciding on a kind of punishment for illegal conduct. Therefore, the DPA considered it doubtful that the processing of personal data within the civil recovery scheme would be lawful. As a result, this scheme has not been implemented.

Liechtenstein

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

One of the tasks of the Data Protection Commissioner *(Datenschutzbeauftragter / DSB)* is to adopt a position on parliamentary bills and regulations that are of relevance to data protection and to verify that they comply with the provisions of Directive 95/46/EC. In 2008 the Data Protection Commissioner issued a position paper on 20 parliamentary bills. Of particular note here, considering their relevance to data protection, are the two partial revisions of the Liechtenstein Data Protection Act *(Datenschutzgesetz / DSG)* and a joint bill for the processing of particularly sensitive data. These are examined in more detail below:

The *first partial revision of the Data Protection Act* should be viewed in conjunction with Liechtenstein's accession to Schengen and Dublin, whose framework also places focus on data protection. This amendment thus concerned above all the structure and organisation of the Data Protection Staff Office *(Stabsstelle für Datenschutz / SDS)*. Up until this point the Data Protection Staff Office formed part of the state administration of Liechtenstein and was under the control of the Department of Justice, and was thus viewed more as an official agency than as an independent institution. In due consideration of the Data Protection Directive 95/46/EC the Data Protection Staff Office failed to meet the conditions for a "completely independent supervisory authority".[34] This complete independence means that the institution of the Data Protection Commissioner must be completely independent in institutional, staffing and financial terms. An adjustment of the Data Protection Act was thus required in order to be as well-prepared as possible for the Schengen/Dublin evaluation. The corresponding changes to the Data Protection Act stipulate that the Data Protection Staff Office *(Stabsstelle für Datenschutz / SDS)* be renamed the Data Protection Authority *(Datenschutzstelle / DSS)* and be assigned complete independence from the Landtag (the national parliament of Liechtenstein). The Data Protection Commissioner is no longer appointed by the government, but is now elected by the Landtag. The Data Protection Commissioner is granted independence in terms of staffing and finances and is granted his own right of appeal. These highly significant legal amendments came into force on 1.1.2009.

In a *second partial revision of the Data Protection Act* an implementation of the provisions of the Additional Protocol to the Council of Europe Convention on Data Protection was undertaken, together with an implementation of the Data Protection Directive that adhered more closely to the text of the directive. In addition to more minor editorial changes, which had become necessary chiefly due to the experience gained over the previous five years, the aim was to introduce new certification procedures in line with the data protection provisions. These allow for a data protection quality standard – still to be established – to be awarded not only to operational processes and organisational structures, but also to information technology products. The latter will strengthen the self-responsibility of those who own data collections and is sure to help promote data protection. The amendment of the regulations for data transfer, bringing them into line with Directive 95/46/EC, has the same goal. The notification obligation relating to certain international data transfers is to be replaced by a general obligation to exercise diligence by the owner of the data collection. A further new provision is the inclusion of a statutory basis for video surveillance in public places, following the urgent recommendation by the Data Protection Commission for such an initiative in its ruling of April 2008.[35] Thus prior approval must be obtained from the Data Protection Authority before video surveillance can be used in public spaces. This partial revision will come into force on 01 July 2009.

According to *Article 44 Paragraph 3 Data Protection Act* the transitional period expired on 31 July 2007; it is stipulated here that an explicit statutory basis must be present after this date in order to process data collections and personal profiles. The creation of the outstanding and legally required bases for processing of particularly sensitive personal data was, from this point on, performed in a *joint bill*.

[34] Cf. Article 28 of the Directive 95/46/EC ("complete independence").

[35] Cf. below, B.

B. Major case law

The *Ruling of the Data Protection Commission (DSK) of the Principality of Liechtenstein of 07 April 2008* with regard to video surveillance in the pedestrian precinct in Vaduz constitutes a decision that in principle reflects the constitutional requirements made of the state as regards intrusion into privacy[36].

Facts of the case:
By decision of the municipal council taken on 29 August 2006 the Municipality of Vaduz installed video cameras to monitor the pedestrian precinct. Comprehensive, round-the-clock video surveillance was conducted using 16 cameras. With regard to the statutory basis, the Municipality of Vaduz here drew on Article 52, Paragraph 4, Municipality Law[37].

Prompted by a complaint submitted to the Data Protection Staff Office[38], in 2007 the Data Protection Commissioner issued the recommendation to the Municipality that the video surveillance in the pedestrian precinct should be reduced because a proportionate infringement of privacy could not be assumed. Furthermore it was doubtful whether Article 52, Paragraph 4, Municipality Law provided a sufficiently firm statutory basis. The Municipality did not follow the recommendation and the Data Protection Commissioner submitted the matter to the Data Protection Commission for a ruling.

Grounds for the decision:
The comprehensive video surveillance of the pedestrian precinct constitutes a substantial infringement of the constitutionally protected rights to privacy[39] and personal freedom[40] of those passing by. The comprehensive video surveillance of a public space is thus in itself a substantial infringement of the constitutional rights to a privacy and to personal freedom because it is to be regarded as an infringement with a wide range of spread that affects all persons irrespective of any suspicion who enter the video-monitored area, without these persons being guilty of any definite misconduct or having prompted the intrusion through their behaviour[41].

In the opinion of the Data Protection Commission a constitutional right can only be curtailed when it rests on a statutory basis, is in the public interest, is proportionate and does not fully undermine the essence of the protected legal right; these principles are already applicable by virtue of the European Convention on Human Rights.

Correspondingly, the general clause of Article 52, Paragraph 4, Municipal Law is thus regarded by the Data Protection Commission as insufficient, because comprehensive video surveillance of a public space represents a substantial infringement of privacy and an infringement of the constitutional principle of personal freedom and as such requires special legal authorisation. The greater the level of infringement, the clearer the preconditions need to be regulated. The Data Protection Commission thus recommends the creation of special legal authorisation for video surveillance because such authorisation does not exist at present in the Principality of Liechtenstein and video surveillance is playing an increasingly large role[42].

The public interest pursued by the Municipality, i.e. to promote peace, security and order and to prevent actual offences, such as vandalism and damage to property, is indeed undisputed. However, the principle of proportionality[43] is based on the notion that an infringement of a civil right may go no further than required by the public interest. The regulatory measure must be suited to achieving the goal pursued in the public interest. Furthermore, the measure must be necessary with regard to the intended goal, i.e. it should not be implemented if an equally suitable but milder action would suffice for the intended goal. The infringement should only be as required in functional, spatial and temporal terms.

[36] The complete ruling can be retrieved at: http://www.llv.li/entscheidung_der_datenschutzkommission_zur_videoueberwachung_in_der_fussgaengerzone_in__vaduz.pdf

[37] Article 52, Paragraph 4, Municipality Law states: "He (the head of municipality) presides over the local police force and ensures peace, security and order. He issues the required ordinances and imposes fines on the basis of statutory and local police regulations."

[38] Cf. Annual Report 2007.

[39] Article 32, Paragraph 1 of Liechtenstein's national constitution.

[40] Article 8 EMRK.

[41] Cf. ruling of the German Federal Constitutional Court of 23.2.2007, File No 1 BvR 2368/06.

[42] Cf. above regarding A. to the second partial revision of the Data Protection Act.

[43] Cf. Article 4, Data Protection Act.

In addition to the principles of suitability and necessity, a measure must be reasonable, i.e. it must maintain a sensible proportion between the intended goal or purpose and infringement on freedom.

In order to be able to assess the proportionality, the Data Protection Commissioner had addressed various questions to the Municipality of Vaduz before the start of the proceedings. He thus requested information as to whether less extensive measures had been examined, whether the intended goal might not be achieved by the targeted, selective use of cameras at certain 'hot spots', how many events of damage or loss had occurred in the pedestrian precinct before and after installation of the video surveillance and the number of cases in which the video recordings had assisted in clarifying facts and had contributed to identifying the perpetrator, etc. However, the Municipality was unable to answer these questions satisfactorily both before and during the proceedings before the Data Protection Commission.

In its ruling the Data Protection Commission thus confirms the recommendation of the Data Protection Commissioner whereupon comprehensive and continuous surveillance should be reduced in either spatial and/or temporal terms to the necessary degree. The particular question is thus whether 24-hour surveillance, 7 days a week is really necessary or whether surveillance could be reduced to certain days and to certain times. Furthermore it should be investigated whether a targeted, selective surveillance of certain objects would be sufficient in the public interest.

C. Major specific issues

In addition to the intensive preparations for Liechtenstein's accession to the Schengen/Dublin Agreements, further work was carried out by the Data Protection Staff Office in the field of telecommunications and labour. The latter often concerned the monitoring of an employee at the workplace and practices regarding e-mail and the Internet at the workplace. For the first time since the introduction of the indirect right to obtain information according to Art. 34h, Police Act[44], the Data Protection Commissioner was required on request to check whether the applicant's personal data had been processed by the national police force with regard to state security or to investigations for preventive countering of criminal offences and if so, whether this is lawful.

The year under review saw a strong demand for information regarding the permissibility of data transfers in a wide variety of contexts. Some examples can be cited here: first names of deceased persons published (under the heading of post-mortem personal protection); permissibility of transfer of data abroad; examination marks published on the Internet; data transfer following a release from insurance secrecy; citizen addresses published by municipalities.

The chief method of providing information to the public is the website of the Data Protection Staff Office, on which information is posted regularly about topical and/or important themes. The importance of the website as an information medium is reflected in the steadily rising visitor numbers. The number of hits on the website in the year under review totalled 234,646 (8,355 separate visitors). This represented in excess of a fourfold increase in the number of hits in comparison to the preceding year[45].

The most important themes for the year under review were: the obligation to report data transfers abroad, protection of data concerning children, resolutions of the 30th International Conference on Data Protection, social networks and press releases about the 2nd European Data Protection Day. In addition to presenting topical themes, the website also enables interested parties to access guides concerning the interpretation and applicability of the Data Protection Act, known as the 'guidelines'. In 2008 the *Guidelines on the Rights of Affected*

[44] Article 34h, Paragraph 1, Police Act states: "Every person is entitled to require the Data Protection Authority to check whether the national police force is lawfully processing their data within the scope of state security (Article 2, Paragraph 2) or for preventive countering of criminal offences (Article 2, Paragraph. 1(d). The Data Protection Authority informs the requester in an answer with a standard formulation that with respect to him/her either no data are being unlawfully processed or that in the case of possible errors in the data processing it has issued a recommendation for rectification." The stipulation came into effect in 2007, cf. Annual Report 2007.

[45] In 2007 the number of hits amounted to just 54,679 generated by 7,158 different visitors.

Persons were thoroughly reworked and updated, while the *Guidelines on Dealing with Unsolicited Advertising, particularly Spam* were published for the first time. On the occasion of the 2nd European Data Protection Day the Data Protection Commissioner issued the latter guidelines as a brochure and presented this to the major share of enterprises, insurance companies and collection agencies in Liechtenstein that are active internationally. This was accompanied by a questionnaire with a twofold purpose: to discover how the companies deal with the theme of data protection and to intensify cooperation in this area.

Norway

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

In May 2008, the Storting *(Norwegian Parliament)* adopted amendments to the Personal Health Data Filing System Act that will prohibit prying into patient records. Pursuant to section 13a of the Personal Health Data Filing System Act, "it is prohibited to read, search for or otherwise appropriate, use or possess health information processed under this Act unless justified by the healthcare of the patient or the administration of such care, or unless specifically authorised under acts or regulations." Any breach of this provision may entail fines or imprisonment for a term not exceeding three months. The rules have entered into force and are being enforced by the Data Inspectorate.

In December 2008, the Storting adopted several amendments to the Personal Data Act. A new provision, authorising the prescription of regulations, was included in section 3 of the Act. This amendment was necessary to provide statutory authority for planned regulations on access to employees' e-mail.

At the same time, the Data Inspectorate was authorised through an amendment of section 46 of the Act to impose a non-compliance charge for infringements of the Personal Data Act. The Data Inspectorate was already in a position to impose coercive fines for any ongoing breaches of the Act. The non-compliance charge would be imposed when the breach took place in the past.

In addition, a new Section 47a was adopted, according to which the Data Inspectorate can use the National Collection Agency to collect non-compliance charges and coercive fines imposed by the Inspectorate. The Data Inspectorate has not previously used its authority to impose coercive fines, because the resources necessary for the collection of such fines have not been available.

These statutory amendments came into force on 1 January 2009.

In June 2008, the Storting adopted amendments to the Schengen Information System Act (the SIS Act). The reason was that the EU Council adopted two regulations in December 2006 and a decision in June 2007, which jointly form the legal authority for the second generation Schengen information system (SIS II). These legislative acts were implemented into Norwegian law through corresponding amendments to the SIS Act. In addition, some amendments were adopted because of observations made during the follow-up of the EU Schengen evaluation of Norway in 2005-2006. And finally, some amendments were necessary because Norway has chosen to carry out direct searches in the central SIS II when it becomes operative. As a result of this amendment, the Data Inspectorate is obliged to check, upon the request of the data subject, whether his/her data in SIS are correct, whether the rules for access have been observed and whether the information has been registered and used in accordance with the SIS Act. If the information has been entered by another party to the Convention, this check must be made in consultation with the supervisory body of this Convention party. These amendments have not yet come into force.

The new Freedom of Information Act with appurtenant Regulations (adopted in 2007), which was expected to come into force on 1 July 2008, was postponed until 1 January 2009. The new Act was mentioned in the 2007 Annual Report. It follows from the new rules that public bodies that keep e-mail records have to make such records available on the Internet as soon as the public electronic system for this has been completed. Personal names will only be searchable in this system for 12 months. In addition to this, the Act also allows the publication of public case documents on the Internet. However, it follows from the Regulations that certain data may never be published on the Internet. This applies to information that is subject to a duty of confidentiality, sensitive personal data, national identity numbers, personal identity numbers and numbers with corresponding functions, as well as information about the pay and other remuneration of natural persons, with the exception of information about salaries and remuneration to senior employees in the public sector and senior employees or board members of independent legal entities.

The Storting has adopted a new Health Research Act. This Act was mentioned in the 2007 Annual Report, to which we refer for further details. No date has yet been fixed for its entry into force.

B. Major case law

None to report.

C. Major specific issues

Unclear distribution of responsibility and inadequate internal control
Under the Personal Data Act, responsibility for the processing of personal data rests with a controller. Supervisory activities in 2008 revealed an unclear division of responsibility for a number of databases and personal data registers. Inspections carried out also revealed that internal control routines were often unsatisfactory and that data processors were used even though no adequate agreement had been signed with them.

Increasing data exchange between databases weakens data protection
There is a trend towards a growing number of agencies sharing or having access to personal data from other government services and agencies. The objective is often to increase procedural efficiency. In 2008, this was particularly noticeable in the justice and health sectors as well as in the proposed new Population Register Act.

Systems in the justice sector are methodically being developed to allow for greater data exchange at the database level. In the opinion of the Data Inspectorate, this development means that strict requirements must be made to the statutory regulation of police registers. The Data Inspectorate is aware that the Ministry of Justice was working on draft legislation in 2008. The Inspectorate has made specific suggestions for amendments to the new Police Register Act which it considers necessary, for example the improvement of fundamental guarantees such as adequate deletion/sorting of data, access control and duty of confidentiality.

More widespread use of fake surveillance cameras
The Data Inspectorate is more frequently being contacted by people who feel that their privacy is being infringed by surveillance cameras, which upon closer inspection turn out to be dummy cameras, not real ones. The use of such dummy cameras raises difficult matters of principle. In many cases the dummy cameras are positioned in such a way that they would have represented unlawful surveillance if they had been real.

Even if this is not real surveillance, the feeling of being monitored will be real. At worst, a useless plastic camera may have a strong impact on a person's perception of his/her own everyday life. However, as no processing of personal data actually takes place, such use of dummy cameras falls outside the scope of the Personal Data Act.

Chapter Five
Members and Observers of the Article 29 Data Protection Working Party

MEMBERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2008

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 2 915 3501 Fax: +359 2 915 3525 E-mail: kzld@government.bg kzld@cpdp.bg Website: http://www.cdpd.bg	Mrs Goulla Frangou Commissioner for Personal Data Protection (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2nd floor - CY - 1082 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 Mr Viljar Peep 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 Chairman 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 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 Christos Yeraris Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 –Athens - Greece Tel: +30 210 6475608 Fax: +30 210 6475789 E-mail: christosyeraris@dpa.gr Website: http://www.dpa.gr	Mr András Jóri 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 06.69677.1 Fax: +39 06.69677.785 E-mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Website: http://www.garanteprivacy.it
Latvia	**Lithuania**
Mrs Signe Plumina Data State Inspectorate (Datu valsts inspekcija) Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia 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) A.Juozapaviciaus str. 6 / Slucko str. 2, 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 - L - 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 Joseph Ebejer Data Protection Commissioner Office of the Data Protection Commissioner 2, Airways House High Street Sliema SLM 1549 MALTA Tel: +356 2328 7100 Fax: +356 23287198 E-mail: joseph.ebejer@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 6219/20 Fax: ++34 91 445 56 99 E-mail: director@agpd.es Website: http://www.agpd.es	Mr Göran Gräslund Data Inspection Board (Datainspektionen) Fleminggatan, 14 (Box 8114) - SE - 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se, 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 2008

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 Data Protection Office (Datenschutzstelle, DSS) Kirchstrasse 8, Postfach 684 – FL -9490 Vaduz Tel: +423 236 6090 Fax: +423 236 6099 E-mail: info@dss.llv.li Website http://www.dss.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

Mrs. Niovi Ringou
Acting Head of unit
European Commission
Directorate-General Justice, Freedom and Security
Data Protection Unit
Office: LX46 01/02 - BE - 1049 Brussels
Tel: +32 2 295 12 87
Fax: +32 2 299 8094
E-mail: Niovi.Ringou@ec.europa.eu
Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

NE-AC-10-002-EN-C
10.2758/21790

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 978-92-79-13757-0