NE-AC-05-001-3A-C

EUROPEAN COMMISSION

Eighth Annual Report of the Article 29 Working Party on **Data Protection**

Eighth Annual Report

of the Article 29 Working Party on Data Protection

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

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

ISBN 92-79-00816-1

9 789279 008160

Eighth Annual Report

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

Covering the year 2004

Adopted in November 2005

This report was produced by Article 29 Working Party on data protection.
It does not necessarily reflect the opinions and views of the European Commission nor is it bound by its conclusions.

This report is also available in German and French. It can be downloaded from the 'Data Protection' section on the website of the European Commission's Directorate-General Justice, Freedom and Security www.europa.eu.int/comm/justice_home/fsj/privacy

TABLE OF CONTENTS

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

For the Working Party, the year 2004 was characterised by the lasting dramatic conflict between the multiple attempts of European and foreign governments to implement new instruments in their fight against terrorism on one side, and the need to defend data protection principles as an essential element of freedom and democracy on the other side. The measures proposed by the Council, by Member States and by the Commission are activities within both the third and the first pillar. The European Parliament, the Council and the Commission disagree on the legal basis and, consequently, on the procedure to follow. The Working Party is formally part of the first pillar and there is no equivalent body for giving advice in the third pillar. There is a considerable risk that data protection implications will not be fully taken into account. The Working Party hopes that the Commission and Council will react soon on the appeal addressed to them by the European Data Protection Conference in their Wroclaw Resolution of September 2004 and provide for a comprehensive and effective organisation.

The transfer of passenger data (so-called PNR data) by airlines through their reservation systems to the United States' Customs and Border Protection (CBP), which had been imposed on them by the United States, has finally, after lengthy negotiations with the American side, been accepted by the Commission, against a couple of remaining critical observations made by the Working Party. These concerned the amount of data fields, the lack of clear, binding principles for the use of passenger data and the duration of their storage, thus, on the whole, being a disproportional means (WP 87, 95, and 97). The Working Party was satisfied to learn that the European Parliament shares the same critical view. It even sued the Commission before the European Court of Justice, arguing that the agreement included restriction of the passengers' rights protected by the Directive 95/46/EC and, therefore, should not have been passed without its assent. The Canadian and the Australian cases, where different PNR solutions have been found, demonstrate clearly that the Working Party is ready to accept new data streams for security purposes provided that they are shaped in a proportionate way, which means that they meet the security needs with minimal encroachments on privacy rights (WP 85 and 88).

We are facing the same fundamental conflict between freedom and security needs when discussing plans to introduce European-wide preventive retention of all telecommunications traffic data including those on Internet use. But this plan would have consequences not only for persons flying from Europe to third countries. It would also deeply interfere with the daily life of practically all European citizens using telephones or electronic services. A huge amount of information would become available revealing nearly all our contacts, our interests, our life style, our whereabouts, and finally: what we do, what we think, what we feel and thus, who we are. We know that even data processed by banks and other financial institutions with the highest security levels have become the subject of large-scale intrusion and misuse. A general obligation to store traffic data over a long period of time would not only restrict privacy. Such a regulation would also produce new risks for data security and data confidentiality because hackers and other unauthorised persons would be interested in getting access to enormous amounts of sensitive data. Should we create such immense

risks? The Working Party has voiced its reservation based on human rights (WP 99). It is concerned that the difficult political situation in which Europe finds itself in these times could even deteriorate, if decisions strongly affecting all Europeans will be taken without any proper discussion in the public and without a clearly visible democratic procedure both in the Member States and on the European level. Therefore, the Working Party welcomes the position taken by the European Parliament and the Commission that any regulation concerning processing and retention of traffic data has to be subject to a co-decision procedure.

The insertion of biometric features into personal documents is another element of the European reaction to worldwide security threats. The Working Party has clearly defined data protection needs in the case of visa and other travel documents. But this is only a first step into a new era of identification technology. Biometrics regards the human body as a source of data and makes it machine-readable. The Working Party has analysed its implications and has pointed out the options on different levels, as regards the choice of biometric features, the kind of storing these data or derivates of them (templates), the procedure for issuing the documents and for the practical use, in particular the risks of central data storage and the measures against misuse of the data. The whole subject is of utmost importance; what has just been said on a legitimate procedure of decision-making in the case of preventive telecommunications data storage applies in the same way to the introduction of biometrics into documents which our citizens will be obliged to use.

The Working Party has continued to give guidance on sector-specific questions. The use of genetic data is of growing practical importance. The Working Party has formulated a set of principles taking into account legal requirements and good practices. It has also identified a structural problem that will have to be dealt with in-depth later on: the property of genetic data as being the common heritage of a group of persons related through biological bands, which is clearly in contrast with the general view of personal data being related once and only to its bearer, the 'data subject' (WP 96).

Other sector-specific papers have been elaborated on video surveillance (WP 89) and on unsolicited marketing (WP 90). A more technology-oriented paper focuses on Trusted Computing Platforms (WP 86).

In close contact with the industry, a model for layered information notices has been developed, which is designed to make information given to users of the internet about the use of their data understandable and comparable (WP 100). We do hope that this will bring more clearness into the fine print on the web and will enable users to make reasonable choices.

Harmonised enforcement is, beside legal harmonisation, an equally essential part of European data protection. The Working Party has started a long-term programme with an inventory of enforcement practices in the Member States. With this and some other documents the Working Party has corresponded to an invitation by the Commission to contribute to its Work Programme 2003-2004 for a better implementation of the data protection Directive (WP 101).

The members of the Working Party have found it helpful to lay down in a 'Strategy Paper' their own understanding of their role as part of the European institutions, of their mandate, and of the technological, political and economical framework of their work. They also outlined working methods concerning the work inside the Working Party and the co-operation with others. The European Data Protection Supervisor, who has finally taken up his duties, is a new member of the Working Party. Coordination with him has proved to be of particular importance and has produced beneficial synergies. The general impetus is to raise awareness and knowledge on all levels, to help the European institutions to integrate data protection considerations and needs into their decision-making, and to contribute to a uniform, high and up-to-date level of enforcement in the Member States and at EU level. The Working Party wishes to be as inclusive and transparent as possible. Draft Working Papers will be subject to online consultation, wherever appropriate – a practice which has been applied with good success – and the Working Party will try to give the widest publicity to its work and its results. It is the purpose of the Strategy Paper to consolidate the Group spirit and to contribute to its transparency for its counterparts and the public (WP 98).

Peter Schaar
Chairman of the Article 29 Data Protection Working Party

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://europa.eu.int/comm/justice_home/fsj/privacy/

1.1. TRANSFER OF DATA TO THIRD COUNTRIES

1.1.1. Australia

Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines

Australian border protection legislation empowers Australian Customs to risk assess passengers on the basis of their Passenger Name Record (PNR) prior to arrival in and on departure from Australia. This legislation aims at enhancing the security of the Australian border and serves in particular to implement the Government's 2001 election programme to increase national security.

The Working Party advised favourably on the level of protection afforded by Australian Customs with regard to the transfer of PNR data to Australia.

The opinion was given on the condition that the restriction lay down in subsection 41(4) of the Australian Privacy Act excluding the Privacy Commissioner to investigate complaints from non-Australian citizens or residents in relation to requests for rectification would be taken away. The Privacy Act has been changed accordingly.

1.1.2. Canada

Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines

Canada has adopted a number of laws and regulations requiring airlines flying into its territory to transfer personal data relating to passengers and crew members in order to secure the integrity of Canadian borders and the security of Canada. The Canadian API/PNR programme was already under development long before the events of 11 September 2001, because it was considered part of the programmes which could be used to manage Canadian borders better, allowing Canada to identify and focus resources on high-risk travellers, while facilitating the entry of low-risk individuals.

The Working Party considered that the Canadian requirements would create problems with respect to Directive 95/46/EC for a number of reasons. The purposes for which the data would be required were too widely defined and, in particular, went well beyond that needed for fighting acts of terrorism. The Working Party requested a clear and limited list of serious offences directly related to terrorism. The Working Party also considered that the amount of data to be transferred to the Canadian authorities went well beyond what could be considered adequate, relevant and not excessive within the meaning of Article 6 (1) c) of the Directive. The Working Party requested that the data list would be related to the different public interests at stake. Data should only be retained for a short period that should not exceed a few weeks or months following the entry to Canada. A period of six years, as requested by the Canadian authorities, was considered too long.

1.1.3. United States of America

Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)

Further to its opinions 6/2002 and 4/2003, the Working Party issued an opinion in the light of developments concerning the transfer of PNR data to the US, in particular to the 2003 December Communication from the Commission, on a global approach towards PNR and the negotiations between the European Commission and the US authorities. The Working Party recommended the Commission to exclude transfer of PNR data to the CAPPS II programme and any other system capable of performing mass data processing operations. The Working Party drew attention to the lack of legal binding of the US undertakings and requested further limitation of the purposes for which the data would be transferred, a proportionate list of data elements, no transmission of sensitive data, the importance of adopting a 'push' method of transfer, strict limitations on further transfers of PNR data to other government or foreign authorities, specific rights for passenger in relation to information, access and rectification, and proportionate data retention periods.

Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.

Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America

After the adoption of the Commission Adequacy Decision on 14 May 2004, the Working Party issued two opinions. Opinion 6/2004 notes that the Commission only partly took into account the demands made by the Working Party regarding, in particular, the scope of the data to be transferred, their retention period and the way in which they are used. The Working Party drew attention to the two issues on which all parties are in agreement: 'push' and information of passengers. The Working Party called upon the airlines to replace the 'pull' method of transfer with the 'push' method as soon as possible, as it is a matter of general data protection principle that recipients should only be given the data they actually need. The Working Party welcomed the regular checks allowing evaluation of the data protection rules agreed upon with the US. The Working Party also stressed the need to inform passengers properly, in particular the necessity to inform passengers in a homogeneous way, regardless of the airline or the travel agent they use. To this extent the Working Party adopted two information notices, set out in its opinion 8/2004, and called upon air carriers, travel agents and Computer Reservations Systems to use these notices as broadly as possible.

Report on Safe Harbour

The Working Party provided input to the Commission for the preparation of the report, the content of which was discussed in length by the Working Party. Further to the adoption of the report, the Working Party has worked with the Commission towards ensuring that the identified shortcomings in the report are properly addressed so that Safe Harbour operates as intended. Among others, the Working Party held a meeting with members of the Federal Trade Commission to discuss enforcement issues in general and enforcement of the Safe Harbour principles in particular.

1.2 ENHANCEMENT OF COMPLIANCE WITH THE DATA PROTECTION DIRECTIVE

Declaration of the Article 29 Working Party on Enforcement

On 25 November 2004, the Working Party adopted the declaration on enforcement which summarises the outcome of the discussions on enforcement at the subgroup level and at the plenary, and announces joint enforcement actions for 2005-2006 based on criteria contained in this document.

The Working Party has stated that it is convinced of the necessity of moving forward in the direction of promoting better compliance with data protection laws throughout the European Union and that, in this respect, it will make a joint effort to improve the situation.

Opinion on More Harmonised Information Provisions

The opinion on more harmonised information provisions was adopted on 25 November 2004 aiming at simplifying and harmonising the requirements on companies to inform the citizens about the processing of their data. The Working Party in its opinion stressed how important it is to establish a common approach for a pragmatic solution, which should give a practical added value for the implementation of the general principles of the Directive towards developing more harmonised information provisions. The Working Party endorsed the principle that a fair processing notice does not need to be contained in a single document. Instead – so long as the sum total meets legal requirements – there could be up to three layers of information provided to citizens.

1.3. INTERNET AND TELECOMMUNICATIONS

Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC

This opinion focuses on the legal requirements to send electronic communications (e.g. e-mail, SMS, fax, telephone) to natural persons for direct marketing purposes as set forth by Article 13 of Directive 2002/58/EC. In particular, this opinion provides clarification of some concepts used in Article 13, such as the concept of electronic mail, prior consent of subscribers, direct marketing, the exception to the opt-in rule and the regime for communications to legal persons.

Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG)

This working document evaluates from a data protection perspective the work carried out by Trusted Computing Group, an ad hoc industry consortium drafting specifications for a new class of hardware security chips called Trusted Platform Modules (TPM). In addition to emphasising the need to ensure that the design of the new protocols and devices is privacy compliant by default and contains privacy enhancing features, the working paper contains some suggestions regarding the work carried out by the TCG. Among others, the Working Party suggests the creation of a best practices group within the TCG to deal with the data protection issues at stake and develop guidelines and best practices concerning them.

Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.

This opinion examines whether the draft Framework Decision mentioned above is in conformity with the standards of Article 8 of the European Convention on Human Rights. To this end, the Working Party analyses whether the storage of information foreseen by the Draft Framework Decision complies with the criteria that derive from Article 8 to legitimise interceptions of communications. Such criteria are a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention. The Working Party concludes that the mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided in the draft Framework Decision, is not acceptable within the legal framework set in Article 8.

1.4. SCHENGEN/VISA/FREE MOVEMENT OF PERSONS

The Working Party has closely followed the developments in this area, particular attention has been paid to initiatives in preparation in view of the adoption of Community proposals for the establishment of European information on visas (VIS), a new Schengen Information System (SIS II) and requirement for passports and travel documents issued by Member States. The ad hoc subgroup of the Working Party for justice, legal and security matters has conducted work on these issues.

Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)

This opinion, adopted on 11 August 2004, was given following the presentation by the Commission of a draft Council regulation laying down a uniform format for visas and for residence permits for third country nationals presented by the Commission. The Working Party has also taken account of works and initiatives in view of the establishment of the European information system on visas (VIS).

In its opinion, the Working Party stresses the importance that it attaches to maintain a balance between the requirements of public security and the respect of the individual freedoms recognised by Community and national law, which entails that they respect fundamental principles of protection of personal data.

In the first part of the document, the Working Party refers back to its Working Document on Biometrics (WP 80/2003) and emphasises that due to the particular nature of biometrics, the inclusion of biometric information in visas and residence permits, and the corresponding processing of personal data requires that the principles of Directive 95/46/EC be observed. In particular, the opinion points out the need for a clear and precise definition of the purpose for which biometric data are collected and processed, as well as the proportionality of the system. It also reminds that all the appropriate measures have to be put in place to ensure that the data are not used in a manner that is not compatible with the purposes for which the data have been collected and processed.

In the second part of the document, the Working Party examines the questions raised by the Commission's proposal from the perspective of the protection of personal data. It addresses issues relating to the purpose of the measures proposed and of the establishment of a VIS, such as the retention period of personal data stored, the need to comply with information requirements to data subjects at the time of data collection in accordance with principles of Directive 95/46/EC, access to the VIS data base by third countries, or the interoperability of different systems (VIS, SIS, EURODAC) in order to increase their added value and create synergies. The Working Party states that the European VIS database should be under the control of the European Data Protection Supervisor (EDPS), whilst the related national operations should be under the control of the national data protection authorities; in this regard, the co-operation between the EDPS and the national supervisory authorities should be regulated to guarantee the uniform application of the provisions on data protection.

Standards for security features and biometrics in EU citizens' passports

On 18 August 2004, the Chairman of the Working Party sent the Council, as well as the Presidents of the European Parliament and of the Commission, a letter to inform them about the concerns of the Working Party with regard to the mandatory inclusion of two biometric identifiers in EU citizens' passports, as provided for in the proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports presented by the Commission in February 2004. The letter included several concrete proposals to the text presented by the Commission. Most of these proposals have been integrated in the final text of the Regulation adopted by the Council on 13 December 2004.

Later, on 30 November 2004, the Chairman of the Working Party addressed a second letter to the Council, the President of the European Council and the European Parliament's Committee for Civil Liberties, Justice and Home Affairs (LIBE) to let them know the reservations about the inclusion of a fingerprint as a second mandatory biometric identifier in EU passports as provided for in the text formally adopted by the Council. It stressed the fact that the introduction of an additional biometric feature makes it all the more necessary that an efficient, secure and watertight system is in place making sure that the fundamental right of privacy is not endangered.

1.5. GENETIC DATA

Working Document on Genetic Data

On 17 March 2004, the Working Party adopted a working document on the processing of genetic data. One of its main conclusions is that any use of genetic data for purposes other than directly safeguarding the data subject's health and pursuing scientific research should require national rules to be implemented, in accordance with the data protection principles provided for in Directive 95/46/EC. The processing of genetic data should be authorised in the employment and insurance fields only in very exceptional cases provided for by law, so as to protect individuals from being discriminated against based on their genetic profile. The Working Party concluded that it may revisit the working document in the light of experience acquired by National Data Protection Authorities and may decide to focus in detail on specific areas at a later stage, in order to keep in line with the technological developments linked to the processing of genetic data.

1.6. VIDEO SURVEILLANCE

Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance

Following the public consultation to which the Working Party submitted its working document during 2002-2003 (see seventh report, point 1.3.7), the Working Party issued its formal Opinion on the Processing of Personal Data by means of Video Surveillance (ref. WP 89).

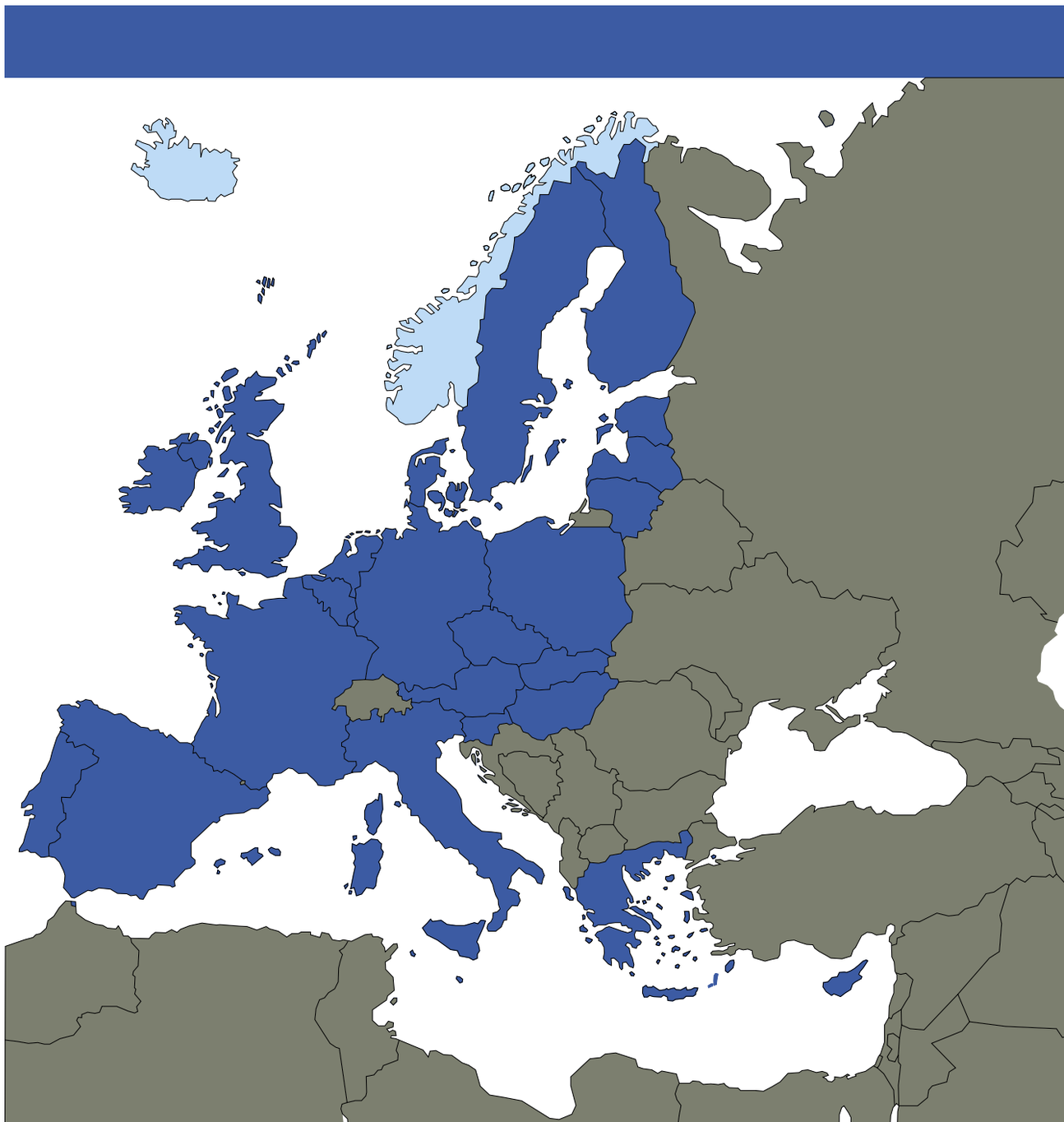
The Working Party has deemed it appropriate to issue this opinion in order to contribute to the uniform application of the national measures adopted under Directive 95/46/EC on the area of video surveillance, due to the growing proliferation of video surveillance techniques and their impact on private life of persons.

The Working Party recalls that, with the exception of those cases expressly set forth in Directive 95/46/EC (i.e. processing operations for the purposes of public security, defence, national security, activities relating to the area of criminal law or those which do not come within the scope of Community law; processing operations by a natural person for a purely personal or household activity, and processing activities solely for purposes of journalism or literary or artistic expression) the processing of personal data by means of video surveillance techniques falls within the scope of Directive 95/46/EC and therefore must respect the principles laid down in the Directive in order to be lawful.

The Working Party also points out that it is fundamental that Member States provide guidance as regards the activity of producers, service providers and distributors, and researchers with a view to the development of technologies, software and technical devices that are in line with the principles referred to in this document.

Chapter Two

Main Developments in Member States



Austria

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

■ The Court Organisation Act was amended (cf. Federal Law Gazette Part I No. 128/2004) creating a special procedure to bring in a complaint because of infringement of data protections rights by organs of the judiciary. This corresponds to the fact that the Austrian Data Protection Commission (hereinafter: DPC) is competent to control the public sector only insofar as neither organs of the judiciary (courts) nor legislative organs (Parliament) are concerned.

■ The Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (in short: e-Government Act) was passed and came into force on 1 March 2004 (cf. Federal Law Gazette Part I No. 10/2004). As a result, legally relevant electronic communication with public bodies is regulated in Austria as follows:

➔ In the context of electronic communications with controllers in the public sector, the possibility of data subjects to access their own data is granted only where the unique identity of the person desiring access and the authenticity of this request have been established. To this end the so-called 'citizen card' was developed, which serves as electronic prove of identity and authenticity in case of any electronic communication.

➔ The most important data protection feature of this system is the fact that the unique personal identification number (hereinafter: sourcePIN) as representative of the electronic identity of an individual citizen is not available to third parties. Controllers in the public sector can only store identifiers which are one-way cryptographic delineations from the (hidden) sourcePIN and are different in the various areas of government activities. Linking data from various sources about one data subject by means of his (single) sourcePIN is thus impossible. Unauthorised capture of sourcePINs is additionally hindered by the fact that the sourcePIN is stored only on the citizen card, which is in the possession of the data subject. The sourcePIN-register is just a virtual register consisting of the (cryptographical) tools necessary to create the sourcePIN for this extra-short moment, which is needed in order to enter it into the citizen card; the sourcePIN is immediately afterwards deleted from the 'register'.

B. Major case law

■ The Ministry of Finance had introduced a new electronic control system of working hours of employees. The beginning and end of working hours could only be entered into the electronic system if the employee was opening his workstation in the office. The time of opening the workstation was used for plausibility controls concerning beginning and end of working hours entered into the electronic system.

■ The Austrian DPC ruled on the inadmissibility of this system on the grounds of disproportionality, because there are many possibilities why an employee cannot start his working day at the office (like attending a meeting outside the office, travelling for business reasons, etc.) so that this system could not be called appropriate for faithfully recording working time.

■ A medical expert examining a person on behalf of a public authority had gained knowledge about possible infirmities of this person relevant for the ability to drive a car and had transferred this information to the authority in charge of drivers´ licences. Upon complaint of the data subject, the Austrian DPC ruled that without specific legal provision allowing the examiner to transfer this kind of information, "overriding legal interest" could not be claimed as a legal basis for data transfers from authority to authority. Considering the serious nature of manifest infirmities of the data subject in the given case, the Austrian DPC found, however, that transmission was lawful on grounds of "vital interests of the data subject", whose life might be in danger when driving a car. Processing sensitive data because of the vital interests of the data subject is allowed according to Article 8 (2) (c) of the Directive 95/46/EC (Section 9 fig. 7 Austrian Data Protection Act 2000).

C. Major specific issues

Deletion from police records

■ In several cases deletion from police records were demanded by data subjects. At the time of these complaints, police records at local level were usually kept in paper files and additionally in index files. Police held that it could not completely erase documentation of their activities, since it is necessary under the Rule of Law to be able to check on police procedures. The Austrian DPC ruled that the purpose 'documentation' might indeed prohibit (complete) deletion of data as long as such documentation is necessary under national law. During this time period, the final outcome of a police procedure would, however, have to be annotated in order to avoid incorrect information. It was moreover ruled that, as far as such information was contained in paper files, Article 12 of the Directive 95/46/EC (Section 27 Austrian Data Protection Act 2000) does not apply; the latter finding was maintained by the Administrative Court and is currently pending at the Constitutional Court.

Right of access to direct marketing data

■ Exercising the right of access to direct marketing data was one of the major problems raised in complaints in 2004. Direct marketing data are a special case as they do not claim to contain correct information but rather statistical information that is 'likely qualities' of a person (e.g. concerning income, interest group, size of household – whether single, couple, etc.). Moreover, the conclusions drawn from the data collected by the marketing businesses are often based on statistical/mathematical models, which constitute the special know-how of the direct marketing enterprise. Having to disclose it in the context of access can raise problems of a fair balance between data protection rights and business secrets.

International data flow

■ Concerning international data flow, the Austrian DPC granted permission to a banking group of companies acting in the Balkans. The permission was given on grounds of unilateral declarations of the group members to follow a set of data protection rules, which was in this case not a special Code of Conduct, as the group chose to adhere to the (non-procedural) provisions of the Austrian Data Protection Act 2000. (The case is documented on the website of the DPC).

Cell phone operators

■ The Austrian DPC has repeatedly dealt with the issue of cell phone operators, screening the credit history of potential customers prior to the conclusion of a contract. As cell phone operators perform services in advance, their need to gain knowledge of the financial situation of potential customers has to be considered as an overriding legitimate interest and is therefore permissible. Since, however, data about credit history are not stored, but included in the decision-making processes as to whether a contract should be concluded, it may be difficult for a data subject to rectify inaccurate credit information. The right to access seems not to cover information about the source of data, which are not stored. It is therefore not always possible to find out from where inaccurate credit information has been gathered and against whom the right to rectification should be exercised.

New register on the status of the citizens' education

■ Wide public interest was given to a new register on the status of the education of the citizens. The main purpose of this register is a statistical one – for this purpose data are kept for 60 years (according to EU statistical provisions). As long as a person attends school (or university) these data are, however, also used for administrative purposes by the school authorities. In order to lessen the data protection implications of such a register containing the whole population, a special scheme for encrypted identification (without storing names) was developed using the social security number of data subjects as an 'entry point'. This fact roused many concerns, resulting in several complaints before the Austrian DPC. The Austrian DPC started an investigation procedure, which has not yet been completely finished. A possible solution will be to adapt the data management in the register to the new Austrian e-Government system of identification and use a special fractional PIN for this register instead of the easily accessible social security number of citizens.

Making identity anonymous

■ It was also brought to the attention of the Austrian DPC that in the publication of a Supreme Court decision the identity of one of the persons involved was not properly made anonymous. Although the Austrian DPC is not competent to control the judiciary, the complaint could naturally be settled to the full satisfaction of the data subject.

Belgium

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

Directive 95/46/EC
No development to report.

Directive 2002/58/EC
The Data Protection Authority (DPA) has been consulted on the draft legislation implementing Directive 2002/58/EC (the law was finally been adopted on 13 June 2005).

The DPA issued an opinion on 14 June 2004, which stresses in particular the following:

■ A general obligation of prior retention of all traffic data, as foreseen by the bill, would be in contradiction with data protection principles as confirmed at several occasions by the privacy Commission, the Article 29 Working Party, international texts and the jurisprudence of the European Court of Human Rights.

■ The draft bill foresees a prohibition of the possibilities to use technical means that would prevent identification of calling ID or tapping of communications, except if these means are used to ensure the confidentiality of messages or the security of payments. The Commission has expressed concern about the fact that such a measure would reduce and maybe suppress completely the possibilities to use means of telecommunication anonymously.

Finally, the draft bill does not transpose Article 13 of Directive 2002/58EC related to unsolicited e-mails. The reason is that this article is considered as being already transposed by a recent law of 11 March 2003 on the Information Society. The DPA has stressed, however, that this law has been elaborated in a consumer protection perspective, and therefore its scope of application is slightly different from the one of the Directive. It applies to 'publicity' instead of 'marketing' e-mails, and thus does not cover charitable or political e-mails. Besides, fax and automated calling machines are not covered. The DPA has called for an official clarification on these points, taking into account the scope of application of Directive 2002/58/EC.

B. Major case law

A major case law related to the possibility of filming workers secretly has recently come to a controversial end. The case started in 2004, with a decision on 24 November at the Court of Appeal of Brussels, which was annulled by the High Court (Cassation) on 2 March 2005. This last decision states that an employer can use, before the court, images of his employee stealing some money while he was filmed secretly (question of compliance with the obligation of information).

These decisions raise two issues:

■ The first issue is about the scope of the privacy law: the judge has decided that the privacy legislation was not applicable (but the collective agreement on video surveillance of workers was) because it was not the employee who was the subject of the surveillance, but the cash register. It could be questioned, in this respect, whether the purpose of the video surveillance was to film the cash register or the employee, to get a proof of his misconduct.

■ The second issue is about the validity of proofs (images) collected in violation of the law and their taking into account in a legal

procedure. It is a question of legal certainty as well, because it will be up to the judge to decide which elements of proof are valid or not, depending on the balance between the interests at stake.

C. Major specific issues

Privacy and transparency of public documents

The DPA faces an increasing number of questions related to the balance between transparency of public documents and privacy. It has stressed that any document including personal data should in principle not be subject to divulgation without the prior anonymisation of the data. If the nature of the document is such that the related person would still be recognisable, then the consent of that person should be obtained before any communication to third parties. The Commission insisted on these conditions especially with regard to the access and re-use by third parties for direct marketing purposes.

Belgian efforts towards a new cyber security curricula better integrating national, cultural and jurisdictional (including privacy) imperatives

The DPA had already decided in 2003 to bring together representatives of the Belgian information security world and Belgian universities, in order to work out together the initial specifications concerning a new cyber security curricula better integrating national, cultural and jurisdictional, including privacy, imperatives. Some fruitful meetings were held and a sensitisation letter explaining the DPA's concerns was sent to the Belgian universities. At the beginning of 2005, a special subgroup was set up within the DPA to specify the next steps of this action. Currently, the work of this subgroup is specifically focused on the elaboration of security guidelines.

Fight against spam

In order to provide a coherent approach to the implementation of the legislation on unsolicited e-mails of 11 March 2003, coordination meetings are taking place at national level between the Data Protection Authority, the Ministry of Economic Affairs and other competent bodies. The objective is to handle and/or redirect complaints in the most efficient way according to their content (fraud, illegal collection of data, etc.).

The results of the 'spam box' experience conducted in 2002 by the Data Protection Authority encouraged the Ministry of Economic Affairs to take an active part the project, in consultation with the DPA.

Cyprus

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

The Law for Processing of Personal Data (Protection of Individuals) came into force in November 2001. The Law was introduced in the context of the harmonisation process and specifically with Directive 95/46/EC of the European Parliament and 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.

At the same time, the Cyprus Parliament ratified the Convention of the Council of Europe for the protection of individuals with regard to the automatic processing of personal data, which came into force on 1 June 2002.

In 2004, the Law regulating electronic communications and postal services was enacted in Cyprus. It transposed, inter alia, the Directive 2002/58/EC on privacy and electronic communications. According to the provisions of section 107, the responsibilities of the Personal Data Protection Commissioner were extended to cover the part of the Law that deals with secrecy of communications, traffic and location data, telephone directories and unsolicited communications.

B. Major case law

Spam

Spam, junk mail and other unsolicited commercial communications increased significantly last year in Cyprus. The Commissioner's Office has been receiving, by phone, a number of complaints every month, mainly concerning unsolicited commercial communications via SMS.

The Law regulating Electronic Communications and Postal Services provides that the use of automated calling systems without human intervention, facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent (opt-in).

The only exception where opt-out can be used is where a natural person or a company/ organisation obtain from its customers their electronic contact details or e-mail, in the context of a sale and may use them for direct marketing of its own similar products.

The investigation of these complaints sometimes presents problems due to constitutional and other legal provisions relating to the right of every person to respect and secrecy of his communications.

The Commissioner is currently engaged in discussions with the ISPs who will undertake to locate the spammers and warn them that if they do not terminate this illegal activity, the ISPs will discontinue the provision of services to them.

Cyprus Stock Exchange

At the beginning of 2004, many complaints were submitted regarding alleged personal data disclosure from the Cyprus Stock Exchange (CSE).

The complainants alleged that the CSE disclosed personal data of their transactions for the period 1999 - 2000 to the Income Tax Authorities.

After investigation, it was found that the Committee of Enquiry, appointed to examine the state of transactions during the years 1999-2000, disclosed the data to the Council of Ministers. The Council of Ministers, based on an Opinion/ advice of the Attorney General, disclosed the information to the Inland Revenue Department.

After examining the provisions of the Mandate of the Committee and the Opinion of the Attorney General, the Commissioner stated that the Council of Ministers was not authorised to disclose any information to the Inland Revenue except in the case of violation by the data subjects of the Income Tax Legislation.

The complainants were informed that they could object to any taxation imposed by the Inland Revenue Department on the ground that the imposition of tax was based on data that had been unlawfully collected/ processed by it.

C. Major specific issues

Public Awareness

Apart from statements to the media on matters of current interest, in 2004 a seminar about the Law on data processing and the obligation of controllers had been organised for the Union of Municipalities and the Association of Accountants.

Guidance on the use of the Internet and video surveillance were issued in 2004 and were also posted on the office website (only in the Greek version) www.dataprotection.gov.cy

The same year, the English version of the law for Data Protection and Part 14 of the Electronic Communications Law, which transposes the provisions of Directive 2002/58/EC, were made available on our website.

More information in the English version will be posted in the website in the near future.

Notifications

Early in 2004, three Municipalities were fined for omitting to submit Notifications for their processing operations/ filing systems to the Commissioner.

Communication

A large number of queries had been received by telephone, both by organisations/controllers and by citizens, regarding personal data processing operations and complaints. Concerning the queries, assistance and guidance was given to help the data controllers to comply with the law. In the case of complaints, the citizens were encouraged to submit their complaints in writing in order to facilitate their investigation.

Audits and Field Inquiries

Five audits had been carried out in 2004. Four of them were routine audits and one was carried out during the investigation of a complaint.

Three public administration departments, one credit referencing agency and one trade company, were selected for the routine audit.

Czech Republic

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

The new modern general Data Protection Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Related Acts (hereinafter: Act 101), almost entirely implementing Directive 95/46/EC went into effect on 1 June 2000. The provisions establishing the Office for Personal Data Protection endowed with all necessary powers and functions of an independent supervisory authority were also embedded by Act 101. Nevertheless some slight alignments were still needed and full compliance with the Directive was accomplished in 2004 when Act 101 was amended by Act No. 439/2004 Coll. enforced on 26 July 2004.

In 2004, the Czech Republic did not succeed in implementing Directive 2002/58/EC as a whole. Only provisions on unsolicited communications were partly transposed by Act No. 480/2004 Coll., on certain information society services, which came into force on 7 September 2004. This Act confined to the Office for Personal Data Protection new strong competence in the fight against unsolicited commercial communications, including the power of imposing direct sanctions. The transposition of the remaining major part of the Directive, together with several other Directives from the 'new telecommunications packet', was drafted by preparing a new act on electronic communications. Having passed through a quite difficult legislative process, the Electronic Communications Act No. 127/2005 Coll. went into effect on 1 May 2005.

In 2004, the Office was also entrusted with stronger competence pursuant to the amendment to Act No. 133/2000 Coll., on Register of Population and Birth Numbers (Act No. 53/2004 Coll., amending some laws related to the area of population registers), in matters involving unauthorised management of national identifiers (the so called 'birth numbers') or unauthorised use of the birth numbers.

B. Major case law

The Office for Personal Data Protection is authorised to render decisions on measures for remedy or/and on penalties. This is without prejudice to anybody's right to refer a case directly to the court or to appeal against a decision of the Office to the court.

Several judicial proceedings involving the Office for Personal Data Protection as a party to a lawsuit were closed during the year. No decision is unfavourable to the Office. As an example, one decision has been made on a constitutional complaint lodged by the Czech Statistical Office (CSO) against the Office for Personal Data Protection in 2002 in relation to the prohibition to process certain personal data obtained during the census of the population, houses and apartments. The Constitutional Court rejected the complaint and it thus holds that the CSO may no longer use certain data from the census and these data are permanently blocked.

Three decisions of the Office for Personal Data Protection on imposing a penalty were challenged by an administrative action. Two actions have already been decided by a senate of the Municipal Court in Prague in favour of the Office; the Court found no defects in the procedure of the Office in imposing the penalties and fully upheld its legal argumentation.

C. Major specific issues

In 2004, certain areas caused special concerns and fears of the Office about high risk of infringement on the privacy of individuals from the viewpoint of protection of their personal data, for example:

- electronic communications and telecommunications (interceptions, retention of processing data, unsolicited commercial communications)
- video surveillance (camera) systems
- land registry and other publicly accessible registers
- new technologies – RFID, biometric data
- healthcare and social sectors.

In 2004, the Office held 35 proceedings that issued into decisions on imposing a fine. Two examples with the highest validly of imposed fine are as follows:

■ An employment agency: A fine of 500 000 CZK (about € 17 000) was imposed on an employment agency, which, as a controller of personal data of applicants for employment, processed their sensitive personal data without having their express consent to such processing and, furthermore, failed to ensure in processing these personal data that the data subjects did not incur any harm to their rights, particularly the right to preserving human dignity. The agency also failed to adopt any security measures relating to the processing. The administrative proceedings against this company were commenced based on the discovery near municipal waste bins of written documents containing personal data of applicants for employment. These written documents contained numerous personal data of applicants, including sensitive data on their state of health, lack of criminal record and nationality, and also written assessment of the applicants by consultants and employees of the employment agency, which contained various subjective, abusive or even gross remarks on the applicants. This case was finally closed when the Municipal Court in Prague rejected a petition against the administrative decisions.

■ A bank: A bank, as a controller of personal data, in the framework of a campaign aimed at obtaining new clients, collected and subsequently processed personal data of the potential clients, without fulfilling, with respect to these persons, the notification obligation of a controller. Furthermore, with respect to some personal data, it was not able to demonstrate the consent of the data subject to the processing of personal data. It followed from the control findings of the Office, that employees of the bank were requested to collect personal data of their friends or business partners. They were motivated to such conduct by non-financial remuneration, provided that inadequate activity of certain employees in this area resulted in a request for fulfilment of the set task, which amounted, in some cases, to a threat. A fine of 485 000 CZK (about € 16 000) was imposed on the bank for mentioned breach of the duties stipulated in the Personal Data Protection Act.

Denmark

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

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

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

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

- The Danish Constitution
- Law on Marketing Practices, Section 6a (cf. Law No. 450 of 10 June 2003)
- Law No. 429 of 31 May 2000 on Processing of Personal Data
- Law on Competitive Conditions and Consumer Interests in the Telecommunications Market (cf. Exec. Order No. 661 of 10 July 2003), Section 34
- Executive Order No. 666 of 10 July 2003 on the Provision of Electronic Communications Network and Services
- Chap. 71 of Law on Administration of Justice, cf. Exec. Order No. 777 of 16 September 2002
- Section 263 of the Penal Code, cf. Exec. Order No. 779 of 16 September 2002.

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

■ In 2004, the DPA had focused a great deal on the upcoming reform of the structure of the public sector. Among other issues the DPA commented on several legal initiatives – 29 out of 226 new bills sent to the DPA are related to the reform.

One of the elements in the upcoming reform is the establishing of the new Public Service Centres which will give citizens a more direct access to their local public authority. In that regard, the DPA noted that, among other things, the issue of which authority was the data controller should be clarified before the centres are established and of how the necessary security precautions were to be maintained cf. the principles of Article 17 of Directive 95/46/EC. Furthermore, the DPA raised the need to provide the relevant employees handling personal data with sufficient training regarding data protection standards.

■ The DPA was asked to comment on a bill introducing changes to the Act regarding a Central DNA-profile Database. The purpose of the bill was to expand the possibility of using the DNA-profile database in the investigation of crime.

Among other things the DPA found that the expansion would imply a relaxation of the terms of registration previously set for the database, and a much larger amount of biological data than before would be collected. With this information, the DPA expressed doubt, whether the necessary proportionality was present between the purpose of the bill and the amount of biological data and the time of data retention.

■ The DPA was also asked to comment on a bill implementing a duty for public authorities and private organisations to obtain a so called 'child certificate' before engaging a person who is to work with children under the age of 15. These certificates involve information on whether the data subject has ever been convicted of a sexual offence in relation to children.

The DPA noted that the written consent of the data subject must be present before the child certificate can be obtained.

The DPA was, in lieu of the principles of data protection and privacy, concerned by the fact that information about serious criminal offences risked being spread out to such a large number of private organisations, and by the fact that these child certificates were to be obtained without an assessment of the necessity in each case. The DPA also raised questions about the duty to notify to the DPA cf. Articles 18-20 of Directive 95/46/EC.

The DPA was generally of the opinion that the implementation of a general duty to obtain these certificates for such a large number of people, should only take place if it was found that substantial public interests would be served hereby.

B. Major case law

■ In 2004, the DPA held that a large supermarket chain's practice of checking credit information for all their employees over the age of 18 gave rise to certain data protection issues. The DPA was of the opinion that section 5, subsections 1-3, (implementing Article 6 of Directive 95/46/EC) sets certain limits about in which cases credit information about an employee can be obtained. The DPA therefore found that, following the coming into force of the Danish Act on the Processing of Data, credit information data may only be obtained regarding employees holding positions of particular trust. In that regard, the DPA found that positions, for example of a more practical nature, cannot be considered to be positions of particular trust.

■ In connection with a complaint concerning the right of access to personal data, the DPA declared that the processing and retention of communication from a chat-site could only take place with the explicit consent of the data subject. The DPA also found that this data could be stored for up to a year, given that the purpose of processing this data was to maintain a safe environment on the website, and to assist the police in cases where indecent behaviour towards children had taken place online.

■ The DPA also expressed its opinion on the processing of data in relation to the US Sarbanes Oxley Act, which requires accountants to register with the PCAOB (Public Company Accounting Oversight Board). The information is made public on PCAOB's website. The processing was based on consent from the data subject.

The DPA was of the opinion that the processing did not live up to the general principles contained in Article 5 of the Act on Processing of Personal Data (implementing Article 6 of Directive 95/46/EC), and that consent given by the data subject could not be sufficiently specific and informed, as required by Section 3 subsection 8 of the Act on Processing of Personal Data.

In summary, the DPA did not find the necessary proportion between the amount of information disclosed and the purpose of the registration with PCAOB, also considering the fact that the information was to be publicised on PCAOB's website.

C. Major specific issues

In 2004, the DPA directed focus towards the so-called head-hunter companies, after it had surfaced in the media that many of these did not have the required authorisation from the DPA.

The DPA contacted approximately 300 companies, giving them a brief description of the rules in the Act on Processing of Personal Data, and requesting that they apply for authorisation if applicable.

The result was almost 250 applications by the end of 2004. Besides authorisations, the DPA also directed several resources to informing the companies of the Act on Processing of Personal Data, with specific attention to the rules concerning consent from the data subject and data retention.

It is the opinion of the DPA that the lack of applications in this area is due to ignorance of the rules of data protection, and the purpose of such a targeted effort is therefore to create awareness of the rules in the industry. A positive side effect of the effort is the rising number of applications from related industries, for example temporary employment agencies.

Estonia

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

During the last year there have been no changes to the new version of the Personal Data Protection Act (PDPA)[2], although the Government of Estonia is planning amendments for the PDPA and the workgroup has already been constituted.

In August 2004, the Government enacted new security measures for information systems[3].

The regulation enacts usable information systems and related security measures systems in the maintenance of state and local governments' databases. The security measures system consists of the regulation of specifying security requirements and the description of the data's organisational, physical and info-technological security measures. The regulation comprises the description of security classes and levels. Security classes are divided into four components: time criticality, severity of consequences of delay, integrity and confidentiality.

B. Major case law

During 2004, the Estonian Data Protection Inspectorate (EDPI) was involved in two cases that found their way to the Supreme Court. Both of them were with regard to access to public information. The first one concerned the EDPI and the Estonian Tax and Customs Board. The case involved the Board's register of documents and the restriction on access[4]. The Supreme Court upheld the previous judgments of the Administrative Court and Circuit Court.

According to Court, the complaint made by the Board fell outside the competence of the Administrative Court. Thus the decision made by the EDPI (that the restriction is illegal) was not proceeded with by the courts. In November 2004, the restriction on access was made legal with the alteration of the Taxation Act[5].

The second case involved the EDPI and a private individual[6]. The case was about a complaint made by the individual against the EDPI's decision on appeal. According to the EDPI's decision on appeal, the private individual (who was a member of city council) had no right to ask for information about the wages and salaries of the employees of the institutions administrated by the city, because these employees are not public officials. The Supreme Court decided that the private individual wanted to obtain the information as a member of the city council and, on that basis, this was not a request for information under the terms of the Public Information Act[7].

[2] Personal Data Protection Act, available at http://www.legaltext.ee/text/en/X70030.htm
[3] RTI 26.08.2004.63.443, available at https://www.riigiteataja.ee/ert/act.jsp?id=791875
[4] Supreme Court case no. 3-3-1-38-04, available at http://www.nc.ee/klr/lahendid/tekst/RK/3-3-1-38-04.html
[5] Amendment of the Taxation Act, available at https://www.riigiteataja.ee/ert/act.jsp?id=901885
[6] Supreme Court case nr.3-3-1-55-04, available at http://www.nc.ee/klr/lahendid/tekst/RK/3-3-1-55-04.html
[7] Public Information Act, available at http://www.legaltext.ee/text/en/X40095K2.htm

The Supreme Court repealed the previous decisions made by the Administrative Court and Circuit Court and concluded the proceedings, because the employees of the institutions administrated by the city are not officials and their salaries and wages are not public. The EDPI's decision was sustained.

C. Major specific issues

The biggest issue during the last year was the problem concerning personal data processing for scientific purposes.

Estonia's latest version of PDPA came into force in October 2003. According to the Act, the person's consent is required for processing personal data in scientific, historic and statistic researches. In addition, it is demanded to register the processing of sensitive data in Data Protection Inspectorate; this presupposes application of required security measures. This initiated the confrontation between the Inspectorate and scientists.

Opponents take the position that the EDPI and Personal Data Protection Act are unfoundedly inhibiting the processing of personal data. The EDPI finds that the biggest problem is the lack of awareness of processing the personal data (opponents do not analyse the reasons or know why the restrictions for the processing of sensitive data are implemented), but also that there could be other reasons like the lack of resources, knowledge of IT and human rights, and not following the changes of information society.

At the moment, the work group is established to find solutions.

Finland

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

The implementation of Data Protection Directive 95/46/EC

The Directive of the European Parliament, and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999. The Act was revised on 1 December 2000, when provisions on the Commission's decision-making, as well as on 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 implementation of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

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

The responsibility for enforcing the law was divided so that the mandate of the Office of the Data Protection Ombudsman includes:
- regulations on processing location data
- direct marketing regulations,
- regulations on cataloguing services
- regulations on users' specific right to obtain information.

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

Main developments concerning:

■ Legislative measures adopted under the first pillar.

The Act on the Protection of Privacy in Working Life (759/2004) entered into force on 1 October 2005. The new legislation replaced the earlier legislation on the matter. The new law now includes regulations on when an employer has the right to process a document on drug-use testing, how camera surveillance is to be organised in the workplace, and how employees may, in co-operation with their employer, influence matters related to personal data processing.

The new Aliens Act (301/2004) entered into force on 1 September 2004. The purpose of the law is to implement and promote good governance and legal protection in matters concerning aliens. In addition, the purpose of the Act is to promote managed immigration and the provision of international protection with respect to human rights and basic rights, and in consideration of international agreements binding on Finland. The law regulates on establishing family ties by means of DNA analysis. The processing of personal data in the aliens' administration is stipulated in the Act of the Register of Aliens (1270/1997), which was revised with the enactment of the new Aliens Act. The Act of the Register of Aliens includes specific regulations on the processing of personal data in the aliens' administration.

The Statistics Act (280/2004) entered into force on 1 July 2004. The law stipulates the methods and principles of data collection, statistics planning and the methods applicable to the compilation of statistics by government authorities, as well as the obligation to provide information when collecting such data. The law also regulates on the confidentiality, publicity and disclosure of data collected for statistical purposes and the use of such data. The law has further specified the right of Statistics Finland to gather confidential and sensitive personal data based on the obligation to provide information. The law entitles Statistics Finland to disclose personal data to certain bodies in a very few, specifically defined situations. Statistics Finland is the main authority responsible for maintaining national statistics.

- *Changes made under the second and third pillar*

No notable changes.

B. Major case law

The Data Protection Ombudsman received requests to remove from the websites of various bodies personal data relating to other people. These issues were deemed to be primarily considered on the basis of legislation on the freedom of speech and the penal code. Ultimately, protection of privacy in these cases is guaranteed by the regulations on the offences against privacy, public peace and personal reputation, the interpretation of which falls under the auspices of the police and the courts of justice. In general, the Data Protection Ombudsman has regularly dealt with issues concerning publicising personal data on the Internet. With regard to the Asian tsunami disaster, a report was commissioned on the use of the Internet in information provision during a crisis situation, for example by way of releasing the names of the victims on the Internet.

According to the legislation on data protection in electronic communications, electronic direct marketing aimed at a natural person requires by default the prior consent of the recipient of such marketing. However, this consent is not, necessary if the service provider or the seller of a product receives the customer's contact information by e-mail, SMS, voice mail, or multimedia messaging in conjunction with the sale of a product or service, and if the same service provider or seller of the product uses this contact information in the direct marketing of products or services related or otherwise similar to the earlier product or service. The Data Protection Ombudsman has been obliged on several occasions to give his opinion on electronic direct marketing.

For example, the similarity or relatedness of services or products supplied via SMS to previously supplied ones are defined by the content of the service or the purpose of the product, not the device used in the purchase or delivery of the service. For example, if a natural person has purchased a utility service via SMS, it is not permissible to market entertainment services to this person using SMS. Whenever it is possible to target direct marketing to a natural person without his or her prior consent, the service provider or the seller of a product is obliged to provide the customer with the

opportunity to easily, and without any costs, refuse the use of his or her contact information in conjunction with data collection and each e-mail, SMS, voice mail or multimedia message. This opportunity to refuse such use must be informed to the customer in a clear manner.

Questions related to various biometric identification systems have also been increasingly under discussion. In relation to the introduction of the biometric passport, Finland is preparing an amendment to the passport legislation, which will specifically regulate the processing of biometric identification data.

C. Major specific issues

Many data protection issues have been related to the changes in the operating environment: the rapid development of technology, the wide scope of operations, and the challenges these pose to the guidance in, and monitoring of, personal data processing. Outsourcing, networking, the various forms of electronic business, and service and call centres all mean that the actors, as well as the Data Protection Ombudsman, will face increasingly greater challenges to identify the body responsible for the processing of personal data and the roles of the actors participating in processing personal data. For the same reason, data subjects are having increasing difficulty in forming a comprehensive picture of such activities.

This kind of development sets new challenges for the Office of the Data Protection Ombudsman, as it is increasingly more difficult to pinpoint how data protection legislation can be applied in each case. What further complicates the matter is that, in many cases, some part of the service process in question is produced outside Finland, sometimes even outside the EU.

An example of the changing service production chains is location data services. In these services, the data indicating the location of a terminal device managed by the operator is used to produce various value-added services which require – given the consent of the data subject – the disclosure of location data to another service provider.

According to the Personal Data Act, the prosecutor is obliged to consult the Data Protection Ombudsman before pressing charges in a matter concerning a violation of the Personal Data Act. The number of such consultations has increased steeply. The reasons for the increase are:

- citizens' (data subjects') improved awareness of their rights with regard to personal data
- improved awareness of the significance of data protection
- better technical standard of data security in data processing systems, which has enabled a higher success rate in criminal investigations
- the publicity that the nationally significant criminal cases concerning the confidentiality of communications have recently received.

Public awareness of data protection seems to be continually increasing. The Data Protection Ombudsman has endeavoured to influence this development by supporting, within the scope of his mandate, the register controllers in providing even better information to data subjects.

During 2004, the Office of the Data Protection Ombudsman, for the third time, carried out the project with the working title 'the Internet Police'. One of the main target groups for this project is websites offering services that were deemed to contain particularly sensitive data and their administrators. Thanks to this project, some of the brochures were revised and updated. The project emphasised to service providers how important it is to provide the data subjects with the information as stipulated in the Personal Data Act.

In 2004, the first incidences of malicious programs (e.g. Cabir) that spread on mobile platforms were detected. It is one of the Data Protection Ombudsman's duties to provide guidelines in matters of data security. This task was carried out in collaboration with the key data security actors.

The Data Protection Ombudsman is a member of a working group for the Steering Committee for Data Security in State Administration (VAHTI) operating under the Ministry of Finance. The working group prepared the development programme approved at the beginning of this year. Representatives from the Finnish office participated in several projects launched under this development programme. The National Data Security Advisory Board, another significant forum promoting data security in Finland, also continued its work under the auspices of the Ministry of Transport and Communications. The Data Protection Ombudsman is a member of the Advisory Board. One of its features is that is has extensive representation from economic life. One of the central achievements of the Advisory Board, which received wide national and international attention, was the National Information Security Day.

An indication of the increasing importance of the protection of personal data in police activities is the work carried out by Mr Jaakko Jonkka, a one-man committee appointed by the Ministry of the Interior. In his report on the effectiveness of the police performance guidance system and the control of legality within the police, Jonkka suggests that data protection and security related to registers accessed by the police requires special attention. Controlling the use of registers, preventing their misuse, and the problems arising from the shared use of registers in collaboration between authorities are all issues addressed in the report. Jonkka also proposes an objective according to which the police should establish the post of a data security manager or supervisor, reporting either directly to the National Police Commissioner or within the unit in charge of the control of legality.

What is of particular importance is that, in Finland, the scope of data protection work is understood to be very extensive. It is not only a matter of utilising technology; rather, the focus is on education, management, winning customers' trust by means of good and secure services, and other 'soft' approaches. It has been well understood in Finland that while the status of a citizen has changed from being a subject to a customer and that the public has learnt to demand secure operating environments, this development must be evaluated and supported by a wide range of methods provided by the information society, technologies and jurisprudence.

One of the key development areas for 2004 was the updating of the Finnish office's website. The aim has been to make information more easily accessible and to provide more up-to-date and interactive information. The amount of information available on individual cases and international issues has also been increased. As part of this development work, a user survey was carried out in spring 2004. The total number of respondents was 350. The feedback called for a search facility, practical instructions and better structure of the website. The new website was launched on 7 September 2004. The number of visitors is also a useful indicator when evaluating the effectiveness of the activities and the level of awareness in matters of data protection.

France

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

The law of 6 August 2004 transposing Directive 95/46/EC

The French Parliament transposed Directive 95/46/EC of 24 October 1995 into national law by a long-awaited law adopted on 6 August 2004. It was decided to keep the 'Informatics and Freedoms' law of 6 January 1978 but to completely overhaul it. The main principles of data protection remain unchanged, but significant changes were made to the provisions of the law of 6 January 1978 relating to overall structure and philosophy (scope, establishment of a data protection officer and new powers granted to the CNIL).

First of all, there are significant changes in the formal procedures required prior to automated processing.

The first major change is a provision in the new French personal data protection law whereby the declaration obligation of all organisations, both private and public, is relaxed if they designate a data protection officer, who could be called an 'informatics and freedoms officer'. This officer's status and tasks will be specified in an implementing decree. The CNIL made its own contribution to the current discussions on the exact nature of this officer. More generally, the law makes numerous provisions for simplifying the prior formalities, of which the CNIL made extensive use in the past year.

However, conversely, prior controls have been stepped up for various types of processing. Several of these, all of which are specified, concern prior control by the CNIL (opinion or authorisation). For example:

- processing of sensitive data that must be anonymised quickly, or where processing is justified in the public interest
- certain processing of genetic data
- processing of data relating to infringements, court sentences or security measures carried out by copyright companies in order to combat the illegal downloading of Internet files
- data processing that, by its nature, scope or purpose, may prevent individuals from benefiting from a right, benefit or contract in the absence of any law or regulation
- automatic processing of data containing details of social difficulties of individuals
- processing of biometric data needed to control the identity of individuals, etc.

The entry into force of the Law of 6 August 2004 has also led to changes in CNIL's control procedures. The new control policy laid down by the CNIL in March 2004, characterised by the wish to significantly step up on-the-spot checks in order to control processing more closely, anticipated the change in the balance of the legislation relating to control (fewer prior checks, more ex post checks). The Commission must decide which fields of activity will be subject to on-the-spot checks, in order to ensure that the CNIL's decisions and recommendations are followed up, to respond to growing public concern or, more specifically, to ensure that security measures are implemented in order to guarantee the confidentiality of the information processed. Evidently, the CNIL will continue to carry out checks in order to investigate complaints addressed to it by individuals. Without waiting for publication of the implementing decree, in November 2004 the CNIL amended its interior regulations in order to establish control procedures under the new law, in particular

the introduction of reports and the providing of information to the public prosecutor with jurisdiction for the geographical area in question, both of which measures are provided for in Article 44 of the Law. Furthermore, under Article 19 of the amended Law, certain Commission officials are authorised to make checks.

This control policy is also reinforced by the CNIL's new powers to impose penalties under the new law. Until it came into force, the CNIL could only issue warnings to the organisation in question or report the facts to the public prosecutor. The Law of 6 August 2004 gave the CNIL significant powers to impose administrative and financial penalties. The Commission intends to rapidly use all the means of control and coercion available to it in order to ensure that the Law is applied effectively.

There is a wide range of coercive measures and penalties. They include warnings, fines, orders to cease processing and withdrawal of authorisation. Where urgent action is needed, the Commission may decide to temporarily interrupt processing or to block data (for three months) except for certain processing carried out by the Government. In cases of serious and immediate damage to rights and freedoms, the Chairman of the CNIL may ask the judge to order any security measure needed to safeguard these rights and freedoms. For first offences, a fine of € 150 000 can be imposed, or for undertakings, € 300 000 or 5% of turnover in the last financial year excluding taxes, up to a limit of € 300 000 (Article 47(2)). The amount of these fines must be "proportional to the seriousness of the offences committed and the benefit obtained from these offences". Lastly, the criminal penalties laid down by Articles 226(16) and 226(24) of the Criminal Code should not be forgotten. Evidently, the CNIL may inform the public prosecutor of any infringements of the law of which it is apprised. Most of the coercive measures must be ordered, not by the plenary session of the Commission but by a restricted formation consisting of six members (the Chairman, the two Deputy Chairmen and three members elected by the Commission for the term of their mandate).

Implementation of Directive 2002/58/EC

- *The law of 21 June 2004 on the digital economy*

The law on confidence in the digital economy transposing certain provisions of Directive 2002/58/EC was adopted on 21 June 2004. The main innovation introduced by the Law on the Digital Economy is the need for prior consent (opt-in): sending business messages by e-mail, SMS (Short Message Service) or MMS (Multimedia Messaging Services) is prohibited unless the recipient has given consent to receiving this message. This consent must be given with full knowledge of the facts. For example, acceptance of the general sales conditions does not mean that the person concerned has given consent to receiving trade promotions. Furthermore, an individual who has agreed to receive such material must be clearly informed of the identity of the undertaking sending it and must be given the option of asking not to receive any advertising.

Where an undertaking already has a relationship with a customer, the customer's prior consent is not needed provided that the material sent by the undertaking relates to similar products or services to those formerly bought or subscribed to by the customer. In addition, when making an order the customer must be given the opportunity to decline, free of charge, advertising material from the undertaking. Numerous discussions took place in 2004 as to whether prior consent should

be required in trade promotion between businesses (B to B). Although it is not disputed that an e-mail address assigned by a company to its employees constitutes personal data if it enables an individual to be identified, businesses wanted application of the new legislation to be more flexible in business situations. At the beginning of 2005, the CNIL concluded that trade promotions may be sent to individuals at their professional e-mail address without their prior consent provided that the message is sent to them by virtue of their function in the private or public organisation that has assigned this address to them.

- *The law of 9 July 2004 on electronic communications*

A decree of 1 August 2003 organised individuals' rights with regard to universal directories or information services, but left a number of questions unresolved. These included the case of mobile telephone subscribers. The CNIL had considered that universal directories should only contain data of mobile telephone subscribers who have expressly asked to be included in them. This departed from the principle that individuals are included in the directories unless they object. Following a reversal of policy by the players involved, the law of 9 July 2004 on electronic communications finally ratified a position that is in line with the CNIL's wishes by adopting the system of prior consent for mobile telephone subscribers. The postal services and electronic communications code will be duly adapted by a new decree, which must include other adaptations carried out by a task force set up by CNIL. The new decree, which is due to be published in 2005, will provide the following provisions: telephone operators will have to inform their subscribers of their right to be included in a directory (mobile telephone) or refuse to be included in a directory (landline telephone), not to have their full home address included, to have only the initial of their first name included provided there are no homonyms, not to receive direct trade promotions, and not to be able to be identified by a search using only the telephone number (reverse search). If they so request, subscribers can include data on other users of their line and their profession. In practice, telephone subscribers will have six months from the time they are informed by their operator in order to indicate their choice. The first universal directories should appear at the end of 2005.

Other legislative developments

- *The fight against discrimination*

The fight against discrimination on the grounds of individuals' ethnic origin, nationality or religious beliefs became a central issue in 2004. A number of reports and studies have contributed to the debate on the means of guaranteeing the principle of equal treatment for individuals with respect to access to employment or a certain level of professional responsibility, access to housing or to certain services. The National Anti-Discrimination and Equality Authority (HALDE) created by the Law of 30 December 2004 is the most visible illustration of the authorities' wish to act in this field. Given the complexity of the issues relating to the identity of individuals and respect for their rights, the CNIL decided, within the scope of its powers, to contribute to the national debate currently taking place by setting up a task force to study the processing of data relating to racial or ethnic origin.

- *Automated legal file on sexual offenders (FIJAIS)*

Articles 706-53-1 to 706-53-12 of the Criminal Procedure Code, introduced in the Code by an amendment to the law of 9 March 2004, lay down the conditions for registering the perpetrators of certain sexual offences, either automatically or at the express decision of an authority. These provisions also require persons registered in the FIJAIS to provide evidence of their address once a year and report any change of address within 15 days. The most serious offenders must provide evidence of their address every six months. Registration of offenders in the file and the associated obligation to state their address is designed to achieve the twofold objective of this file set out in the Law: to prevent sexual offenders who have already been sentenced from re-offending and to identify these offenders more easily.

- *Experiments with biometric visas in France*

The law of 26 November 2003 on immigration makes provision for the recording, memorising and processing of the fingerprints and photographs not only, as was previously the case, of applicants for residence permits and foreigners in an irregular situation, but also of applicants for visas. Pursuant to these laws, the Minister of the Interior informed the Commission of a draft decree by the Council of State that would authorise, as an experiment and for a period of two years, the creation of a database of fingerprints and digital photographs of applicants for visas at seven consulates and provide for the recording, at some of these consulates, these biometric data in an electronic chip affixed to the visa issued.

The CNIL was consulted on this draft decree and delivered its opinion on the experiment on 5 October 2004. While recording fingerprints in an electronic chip affixed to the visa did not raise any fundamental difficulties provided the appropriate security measures are taken, the CNIL expressed a number of substantial reservations and objections concerning the conditions in which the experiment was to be carried out, in particular the creation of a centralised database.

The implementing decree takes on board only some of the CNIL's observations and recommendations. The objectives of this experiment have been set out and the arrangements will be evaluated; the information processed will not be kept after the conclusion of the experiment if it is decided not to make the arrangements permanent. However, these experimental arrangements are still based on a central database in which the fingerprints of all visa applicants will be recorded, whether or not they obtain the visa requested. The Commission considers that this entails the risk that foreigners whose visa applications are rejected will be stigmatised, even though rejection of an application is a normal administrative procedure which does not necessarily affect the outcome of a new application, and a rejected applicant is therefore not suspect.

- *Personal medical records*

The law of 13 August 2004 on health insurance made provision for the creation of personal medical records. The CNIL was asked by the Government to give its opinion on the draft law and did so after a debate on 10 June 2004.

The law states that personal medical records are to be kept in accordance with the principle of medical secrecy. The records will contain all the data collected or generated in relation to

preventive care, diagnosis and treatment, in particular to that needed in order to monitor the provision of medical care. Access to personal medical records is controlled, and the law prohibits any marketing of medical data.

B. Major case law

The legal follow-up to the 'Spam Box' initiative

In October 2002, following its 'Spam Box' initiative, the CNIL informed the public prosecutor of five companies that were sending unsolicited bulk e-mails of advertising material ('spamming'). In a judgment of 18 May 2005, the Paris Court of Appeal imposed a fine of € 3 000 on a company that obtained e-mail addresses on public Internet sites on the grounds that it had obtained personal data by illicit or unfair means.

A landmark case: the sentencing of a French spammer

On 5 May 2004, the Paris Commercial Court sentenced a French company for spamming following a complaint lodged jointly by Microsoft, the provider of the free e-mail Hotmail, and the Internet access provider, AOL France. They accused the company in question of having used their services to send a million unsolicited e-mails advertising football-related items via several of its sites.

The judge ordered the company to pay € 10 000 damages and € 12 000 costs. He also prohibited it from sending unwanted e-mails using services proposed by the companies that brought the action.

Germany

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

In the main, Directive 95/46/EC has been transposed into German law. However, Directive 2002/58/EC has been implemented under German law in part only. The new Telecommunications Act entered into force in June 2004. When amending the Act, the Bundestag suggested that traffic data should not be kept specifically for the sole purpose of law enforcement by the competent authorities. The new act lays down regulations on:

- the mandatory registration of holders of prepaid SIM cards
- the use of data concerning the location of mobile phones
- the possibility of obtaining both the identity and the address of a person from a calling number (reverse directories).

The Directive has not yet been implemented in the field of tele- and media services.

B. Major case law

Federal Constitutional Court ruling of 3 March 2004 on acoustic surveillance of living quarters (BverfG 109, 279)

The Constitutional Court has ruled that significant sections of the provisions of the Code of Criminal Procedure that relate to the acoustic surveillance of living quarters are in breach of the Constitution because they violate human dignity. The acoustic surveillance of living quarters for purposes of prosecution under criminal law must not impinge on the core of private life, which is subject to absolute protection. Moreover, procedural safeguards – particularly the ex post notification of the persons concerned – must be guaranteed where undercover investigation methods are used, as with other techniques. A new set of rules on the provisions governing criminal proceedings, designed to implement the ruling, was adopted on 17 June 2005. They were to enter into force on 1 July 2005.

Ruling on the Law on State Security Service (Stasi) documents

Under the first ruling by the Federal Administrative Court of 8 March 2002, the federal official responsible for the documents of the former GDR State Security Service was absolutely prohibited from publishing the documents relating to the case of former Chancellor Helmut Kohl against the latter's will. However, there was again some doubt about this after the adoption on 6 September 2002 of the new version of the clause on weighing up comparative merits in Section 32 of the Fifth Act amending the State Security Service Documents Act of 6 September 2002. The parties involved had again brought the case before the courts for clarification.

The Federal Administrative Court's second ruling of 23 June 2004 stipulated that the amended State Security Service Documents Act was to be interpreted and applied restrictively in accordance with the Constitution. The Court laid down a number of criteria for this purpose. The federal official responsible for the documents of the former GDR State Security Service has revised her internal guidelines on the publication of files and amended practices accordingly. As a result, the publication of documents without the consent of the person concerned is now subject to even more careful checks and is only possible in very, exceptional cases only.

C. Major specific issues

Storing data on nationals of EU Member States in the Central Register of Foreign Nationals

The issue of whether data on nationals of EU Member States resident in the Federal Republic of Germany can be stored in the Central Register of Foreign Nationals (AZR) and whether such data storage is compatible with Directive (EC) 95/46/EC on data protection has not been finally clarified. The Federal Ministry of Home Affairs has not so far responded to repeated demands by the federal official responsible for data protection for a ban on the storage of such data generally.

Stepping up co-operation between the security authorities on combating terrorism

Co-operation between the German police and intelligence services to combat international terrorism has been stepped up.

An important element in this new security structure is the anti-terrorism centre set up in Berlin in December 2004. There is ongoing co-operation in two separate evaluation and analysis centres between special units and units responsible for analysis belonging to the police and intelligence services, the aim being to assess possible dangers and analyse the potential for Islamist terrorism in terms of the people who might be involved.

A further aspect of the intensified co-operation between security authorities is the planned administration of joint project databases to which the police bodies and intelligence services will be given on-line access – including read and write functions – in the context of an evaluation project.

Finally, discussions are underway on the establishment of a shared index file, to include references to items of information stored in police or intelligence service repertories. This type of co-operation is defensible from a data protection angle provided that the German constitutional rule is respected that separates the police from the intelligence service and determines the limits to co-operation on information matters. This means there must be strict compliance with the rules in force on duties, powers and transfers. The services involved may be granted the power to store personal data in a joint database, if and only if they are permitted to supply the data to be entered to all other services involved, in accordance with the applicable provisions on its transfer.

Greece

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

Directive 95/46/EC

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

In 2004, by decree of the Minister of Justice, a special committee was created for the revision of the above law. The revision was decided mainly in order to comply with the first report of the European Committee in regard with the implementation of the Data Protection Directive.

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

Directive 97/66/EC

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

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

Directive 200/58/EC

The procedure for the implementation of Directive 2002/58/EC into national law is not completed yet. A Law-Project for the implementation of Directive 2002/58/EC on data protection in electronic communications is going to be submitted by the Minister of Justice to the Parliament for adoption in September 2005.

Main development:

- *Legislative measures adopted under the first pillar*

No major developments to be mentioned.

- *Changes made under the second and third pillar*

Schengen Evaluation

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

B. Major case law

Opinions 1, 2 & 3/2004

Parliamentary control and the right to data protection are both guaranteed by the Constitution. Accordingly, the access of Members of Parliament (MP) to public documents in order to accomplish their tasks must be accomplished in a way that minimises the risks of violation of the data protection right. To that purpose, the requesting MP can have access in situ to the necessary documents but cannot ask for the submission to the Parliaments secretariat of copies of an entire database.

Decision 6/2004

Pursuant to a request submitted by the Socialist Party (PASOK) concerning the notification of a

database of the 'friends' of the party, which was intended to be created during the national congress of the party in which not only its members but also its 'friends' were invited to vote, HDPA judged that the quality of 'friend of a political party' is a sensitive data and its processing is not legal because it may lead indirectly to the violation of the right to secret voting.

Decisions 28/2004, 63/2004 & 58/2005

■ By decision 28/2004, HDPA gave the conditions under which the Hellenic Police had the right to install CCTV in public areas in the city of Athens and its suburbs for the security of the Olympic Games 2004.

■ By decision 63/2004, HDPA accepted the request of the Hellenic Police to extend for six months the period of lawful use of CCTV, which expired after the end of the Olympic Games, for the sole purpose of traffic management but under strict conditions; microphones and all cameras that had been installed for purposes other than traffic management had to be removed; the police were obliged to switch off the system during demonstrations, etc.

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

Decision 61/2004

The intervention of the employer in the electronic communications of the employees constitutes processing of personal data and is illegal if the employee was not previously informed about the possibility of such interventions even for technical reasons, and if he has was deprived of the technical means of using special software to protect the secrecy of his own communication.

Decision 67/2004

As according to Article 9 of the Greek law on data protection, transfer of personal data to third (non-EU) countries presupposes a prior permit by the DPA, the relevant permit was issued to Olympic Airways concerning the transfer of PNR data to CBP office of the USA under the conditions of the relevant Agreement between the EU and USA and the European Council's decision, after prior written information of the passengers according to the relevant opinion of Article 29 WP.

C. Major specific issues

As the number of personnel of HDPA was very restricted and not sufficient to fulfil its important tasks properly (seven legal auditors and five IT experts), the Minister of Justice accepted the proposition for the recruitment of 14 more auditors (eight lawyers and six IT experts) as well as five more administrative staff. The procedure is planned to be completed in autumn 2005.

Hungary

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

Directive 95/46/EC

The state must be transparent, but its citizens should remain non-transparent to it – this ideal was first affirmed in 1989 by the Constitution of the Republic, which recognised the protection of personal data and freedom of information at a constitutional level, the first in Central and Eastern Europe. Since that time, the Constitutional Court has been giving content to these principles and then the Parliament adopted the Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest.

On 1 January 2004 a new amendment entered into force for the better implementation of the EU Directive 95/46/EC. The English version of the Act can be found under the following address: http://abiweb.obh.hu/dpc/index.htm

Directive 2002/58/EC

A part of implementation of Directive 2002/58/EC was completed in 2004. Relevant provisions were amended in connection with unsolicited commercial communications in the Act CVIII of 2001 on specific issues of electronic commercial services, and services related to information society that came into force this year. This means that in case of breach of the provisions by the advertiser, Act LVIII of 1997 on Business Advertising Activity is applicable.

Another act which was amended according to Directive 2002/58/EC was Act C of 2003 on Electronic Communications regarding data processing in the telecommunication sector.

Main developments:

- *Legislative measures adopted under the first pillar*

All bills and proposed modifications to legal instruments having data protection regulations or implications shall be sent to the Data Protection Commissioner requesting his opinion. The appendix of the annual report, which is only available in Hungarian, always contains the list of the bills and modifications to legal instruments sent to the Data Protection Commissioner.

- *Changes made under the second and third pillar*

As Hungary entered the European Union on the 1 May 2004 a number of legal instruments had been modified because of the membership. Besides these modifications, the following changes are considered important:

➔ The Hungarian Parliament enacted the Convention on Cybercrime of the Council of Europe (Act LXXIX of 2004).

➔ The Hungarian Constitutional Court in its Decision 44/2004, relating to the regulations of Act XXXIV of 1994 on the Police, has further elaborated the meaning of the constitutional rights of the protection of personal data and the learning of data of public interest.

B. Major case law

■ The Office of the Data Protection Commissioner launched an on-the-spot inspection countrywide regarding the individual's right to be tested for HIV anonymously. The inspection was provoked by a story run by a weekly newspaper which reported several cases where people were charged for being

tested for HIV and their personal data were also demanded. The colleagues of the Commissioner checked incognito into a number of institutions authorised to administer HIV tests, and reported that a number of them required the personal ID number or the social security number of the applicants. The individual's option to be tested for HIV anonymously, i.e. without having to reveal their personal data, is ensured under § 59 (5) of Act CLIV of 1997 on Healthcare. Patient identification in HIV testing is provided for by the Decree of the Ministry of Health, Social and Family Affairs 18/2002 (XII.28.) on the procedure of administering screening tests and measures to prevent the spread of the infection causing the acquired immune deficiency syndrome. According to the before-mentioned Decree, the cover sheet accompanying the first blood sample in transit to the laboratory shall indicate the medical identification code and number and, separately again, the date and place of taking the blood sample. As the result of the inspection, the Commissioner called on the Chief Medical Officer, as well as the leaders and supervisory agencies of other institutions authorised to administer blood tests under the cited Decree, to allay privacy concerns by offering genuinely anonymous HIV testing. The Commission also called on the interested parties that the consultation principle enshrined in the Healthcare Act must be fulfilled as part of the HIV antibody testing of individuals; so healthcare employees are also liable to advise applicants proactively of their right to get an anonymous test.

■ The Data Protection Commissioner and the Commissioner for Civil Rights conducted a joint investigation with a view to improving the protection of babies left in incubators set up outside the hospital buildings. The Commissioners proposed that the Minister of Justice amend the applicable regulations to ensure the genuine anonymity of the mother resigning her child in this manner by waiving the obligation of the registrar to request a police investigation to determine the identity of children with unknown parents, before proceeding to make an entry in the Registry of Births. This provision was finally overruled by implementing the Commissioners' initiative. Another legal problem was that, by leaving the baby in the incubator, the mother satisfied the elements of the arbitrary alteration of family status, a felony defined in the Criminal Code. For this reason the Commissioners proposed new regulations under which the abandonment of babies in incubators for this purpose would no longer be regarded as a felony. The Minister of Justice concurred with the need for an in-depth discussion with the Commissioners and the Ministry of Health, Social and Family Affairs to unravel the issue's complex implications for social relations and rather sensitive fundamental rights, such as the child's right to life and dignity, or the mother's right to self-determination. After several discussions, the Ministry of Health, Social and Family Affairs advised which provisions had to be amended in order to abolish the felony classification of the abandonment. The Commissioners agreed that the proposed amendments serve the protection of the child's fundamental right to life and human dignity without curbing the mothers' right to self-determination, and supported the implementation at the earliest legislative opportunity.

■ The Data Protection Commissioner and the Commissioner for Civil Right issued a joint recommendation concerning the regulation of ovum donation. They pointed out that there is a contradiction between the Healthcare Act's provision permitting in vitro fertilisation and the same law's exceedingly strict data protection provision, which makes ovum donation impossible in practice. As the Act only permits an anonymous donation it thus prohibits the donation by relatives as well. The Commissioner and the Minister of Health, Social and Family Affairs proposed the amendment of the Act.

C. Major specific issues

Most of the 25% increase in the total number of cases had to do with the significant growth of legislative evaluations, complaints and consultations. It is evident from the figures that the annual number of cases, which has risen steadily for the seven years since the creation of the institution of data protection in Hungary, crossing the psychological limit of 1 000 in 2003, reached another milestone in 2004 when it hit 2 000. This tendency suggests that, on the whole, the individual is becoming increasingly receptive to issues of privacy.

Ireland

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

The EU Data Protection Directive 95/46/EC was fully transposed into Irish law by the Data Protection (Amendment) Act, 2003, which was passed by the Oireachtas (Irish Parliament) in April 2003. The Amendment Act together with the original 1988 Act constitute the Data Protection Acts 1988 and 2003 and are construed together as one Act.

Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector was implemented in Irish law by special Regulations (S.I. No. 535 of 2003) made by the Minister for Communications, Marine and Natural Resources, which came into effect in November 2003. The new Regulations fully transpose the Directive into Irish law. The Data Protection Commissioner is the supervisory body for enforcement of the Data Protection aspects of these Regulations.

There were no further legislative developments during 2004.

B. Major case law

Successful prosecutions were taken in 2004 against two data controllers for not registering (failing to notify) with the Commissioner's office, while a prosecution against a third for failure to answer an Information Notice was not proceeded with as the firm registered following the issuing of the summons. In late 2004, the Office's solicitors were instructed to issue summons to a premium rate service provider for contravention of the unsolicited direct marketing provisions of the Electronic Communications regulations (S.I. 535 of 2003) which transpose Directive 2005/58/EC.

This Office was not involved in any other court proceedings.

The Commissioner made a number of significant decisions, none of which was appealed to the courts. The most important ones were:

- An individual had made a subject access request for personal data contained in reports held by his employer about a complaint he had made alleging bullying and harassment by a colleague. The employer withheld data in relation to the ongoing bullying and harassment investigation. The Commissioner found that this was in accordance with the exemption to the right of subject access, which applies in relation to data which would prejudice an investigation of an offence. He held also that on completion of the investigation, this exemption would not be applicable.

- In another case, the Commissioner ruled that the exemption to the right of subject access which applies in relation to legal professional privilege should not be used as an excuse to seek to restrict access where it cannot be justified.

- The former publisher of the Bar Council's in-house legal diary (the Bar Council is the National Association of Barristers) used the database obtained in connection with that contract to publish a rival publication after they had lost the contract. The Commissioner found that personal data obtained for the purposes of a data processor contract may not be processed subsequently for a different purpose. As the data processor had responded promptly undertaking to comply with the Commissioner's requirements, it was decided that it was not necessary to prosecute.

- Data relating to membership of a political party was used by a local party member to appeal for donations to a charity. Following the Commissioner's enquiry, the party's national headquarters acknowledged that the local member had used the local party database to send out an appeal for funds for the charity. The headquarters accepted that the use of data in this way was a contravention of the purpose limitation and non-disclosure provisions of the Data Protection Acts, 1988 and 2003. In the course of concluding this complaint, the Commissioner advised the party on their obligations as a data controller, particularly concerning issuing guidelines to members who process personal data about the requirements of Data Protection.

- The Commissioner held in regard to the local authorities and their decisions about allocation of public housing that, even where there is legislation providing that information must be made available to the public for the reasons of openness and transparency, this may not always mean that it is appropriate to place personal information on a website. Consideration must be given to the balance required between the right of the public to certain information and the right of the individual to privacy and particularly to whether the desired objectives can be achieved without disclosing personal details.

C. Major specific issues

Research

During the year the Commissioner dealt with a number of issues relating to health and social work research and clarified data protection requirements so that essential research projects could proceed with the necessary safeguards. The Commissioner called for greater awareness amongst health service personnel and researchers of the data protection rules and emphasised to the Health Services that in order to reduce the risk of disclosure of sensitive personal data, research data should be anonymised (or pseudonymised) in cases where personal identifiers are not needed for the particular purpose in hand. He emphasised that privacy-enhancing technologies have a contribution to make in this area and their use needs to be adopted more widely to facilitate necessary health and social research.

A submission was made to the Law Reform Commission who published a Consultation Paper on the question of a national DNA databank (www.lawreform.ie).

Communications traffic data

Due to the lack of progress at national level throughout 2004 on the unsatisfactory legislative basis for the retention of communications traffic data, the Commissioner issued enforcement notices in early January 2005 to three telecommunications companies requiring them, with effect from 1 May 2005, to hold such data for national security purposes for a maximum period of twelve months. Two of the companies appealed the notices to the Circuit Court while the other did not. The Minister for Justice, Equality and Law Reform introduced legislation providing for a three-year retention period. Given that this brought about a statutory basis for retention of the data by the companies and as the Commissioner did not want unnecessary legal costs to be incurred by him or indeed the companies, he cancelled the Enforcement Notices on 7 February.

Public Service Card

The Commissioner made a submission to Government on the Data Protection safeguards needed in the development of a Public Service Card. Indicating that he wanted the project to be successful, he called for clarity on the scope of the proposal (to be confined to the public service only?) and for clarity in relation to the use of the Personal Public Service Number (PPSN) which would underpin it. He recommended that Government:

- specify the totality of purposes for which the card will be used or could be used
- specify the organisations that can process, the types of data that will be stored on the card and the controls that will be in place to ensure that DP rights are respected
- have separate legislation for this programme preceded by full public informed debate
- be open and transparent from the outset and determine what purposes the Card is to fulfil
- it would be too easy to create the card and then add new purposes later, an approach which could cause Data Protection difficulties.

Privacy statements on websites

During 2004 the Commissioner conducted a survey of Public Sector websites. Altogether, 242 sites were identified and contacted in respect of their use of Privacy Statements. Where organisations collected personal data on-line and/or used technical features, such as cookies, the Commissioner expected that the organisations concerned address this deficiency and that sites would contain an adequate privacy statement by no later than 31 January 2005. This matter is currently being reviewed. In all, the survey showed that 53 sites had adequate Privacy Statements; 46 had inadequate content in their Privacy Statements; 8 had poorly positioned Privacy Statements and 135 had no identifiable Privacy Statement. The Commissioner's Office is in the process of contacting those sites identified as having problems with their Privacy Statements and those with no statements.

Education and awareness

The Commissioner's Office engaged in several public awareness initiatives and a six-week campaign of advertising on buses and trains in the autumn was well received.

Italy

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

The consolidated Data Protection Code (legislative decree no. 196/2003) came into force on 1 January 2004; the Code was brought about through the implementation of both Directives. As explained in the Seventh Annual Report, it was amended by an Act of 26 February 2004 in connection with data retention for the purpose of detecting and suppressing criminal offences. The Act replaced the text of Section 132 in the Code by extending the retention period for telephone traffic data, which may now be retained for 24 months. Upon expiry of this term, they shall be retained by the telecom provider for an additional 24 months, exclusively with a view to detecting and suppressing some very serious criminal offences, including those related to terrorism.

Another amendment to the Code was introduced in March 2004 concerning notification requirements. The data protection Code requires notification of the processing operations liable to affect data subjects' fundamental rights and freedoms that are listed in the relevant Section (37); however, it also empowers the Garante to add to or reduce the list of notifiable processing operations. By the decision adopted in March, the Garante exempted controllers from notifying some processing operations that were considered not to be liable to affect the data subjects' rights and freedoms among those listed in Section 37 – by having regard either to the capacity of the data controllers or to the purposes of the processing.

Reference should also be made to the adoption of general authorisations applying to the processing of sensitive data by various categories of data controller. Under the data protection Code, processing of sensitive data by private entities is allowed with the data subject's consent and the Garante's authorisation, which may also be granted in the form of a general authorisation addressed to categories of data controller – setting out the framework within which the sensitive data at issue may be processed. Seven general authorisations have been issued so far, starting in 1998; their scope of application is time-limited, as they are reviewed regularly to take account of supervening developments. Those issued in 2004 will expire in December 2005.

Other legislative developments:

■ Regulations issued in February 2004 set out the mechanisms for the issuance of the so-called 'Services Card', which is meant to simplify electronic access by citizens to public administrative services, i.e. in view of e-government enhancement. The card will contain the holder's identification data and tax ID code, but no biometric data.

■ The 2004 Budget Act provided expressly for introducing an ad-hoc electronic 'medical' ID card (containing the holder's tax ID Code) to be used by citizens for accessing all National Health services; the relevant provisions were set out in Section 50 of Act 326/2003 and specified subsequently via regulations issued in 2004. This measure was only meant to facilitate supervision over healthcare expenditure, with particular regard to the costs for drug prescriptions. The card is expected to be delivered to all Italian citizens by the end of 2005.

B. Major case law

The Italian Court of Cassation (Supreme Court) issued several decisions in 2004 concerning personal data protection. Reference can be made in particular to the following:

Civil Law

An important decision was reached in a case relating to a request for access to evaluation (scoring) data lodged by an employee with her employer. This request had been rejected by the employer; the applicant had subsequently lodged a complaint with the Garante, which had granted it and ordered the employer to disclose the data. The employer had appealed against the Garante's decision with the competent First Instance Court, which had cancelled the Garante's decision alleging that the operations required to finalise the scoring – although entailing the processing of personal data, and possibly additional evaluation activities – did not fall within the concept of 'personal data'. Additionally, the First Instance Court had questioned the Garante's locus standi in the proceeding in question. The Court of Cassation re-affirmed two important principles in its decision (February 2004) – namely, that evaluation data are personal data, and therefore may be accessed by data subjects pursuant to the right of access provisions irrespective of the time at which they are processed, and that the Garante has locus standi if the case at stake concerns lawfulness of a decision adopted by the Garante with a view to establishing the public interest it is required to safeguard under the law.

In another decision of June 2004, the Court ruled explicitly that the protection afforded to personal data under the law also applies to 'non-structured' data contained in a database as well as to the data taken from public sources. The case had been brought before the Court by some journalists from the public TV broadcasting corporation, RAI, and the company itself in connection with the decision by which a First Instance Court had rejected their claim against the publisher of a daily newspaper; the latter had published news containing personal information on the said journalists, who had requested the information be erased pursuant to the data protection law because it had been processed unlawfully. The Court stressed that the data protection legislation is aimed at safeguarding individuals and their fundamental rights, which may be infringed by processing operations consisting merely of dissemination, irrespective of the data being subsequently included in a structured file system. In assessing lawfulness of a processing operation, account should be taken of all processing activities involved in order to ensure that they do not give rise to substantive breaches of fundamental rights. Additionally, the Court ruled that the scope of data protection legislation goes well beyond private data and information, and also extends to publicly available and/or publicised data, as "any entity processing such data and information can extract additional information by matching, comparing, analysing, linking, etc. the said data, and such additional information has 'informational added value' that cannot be derived from the individual data units considered as such and may potentially violate the data subject's dignity – which is the fundamental value to be safeguarded by data protection legislation".

Criminal Law

In a case concerning the harassment caused by a man to his former fiancé via both SMS messages and posting of images on the Internet, the Court stressed that in the consolidated Code on data protection, which replaced the previous data protection Act no. 675/1996, the fact of causing 'harm' is an intrinsic culpability condition, i.e. it compounds the offence that is typified in the relevant provision. This means that processing sensitive data without the data subject's consent – which is the offence at issue in Section 167 of the Code – does not amount to a criminal offence if no harm is caused to the data subject.

In another decision of July 2004, concerning the processing carried out by a member of a humanitarian relief association whereby a confidential mailing list was used without the recipients' consent to send electoral propaganda material, the Court better clarified the 'harm' concept referred to in Section 167 of the Code. The Court ruled that the fact of causing 'harm', which is to be regarded as an objective punishable condition, is criminally irrelevant if minimal harm is caused to the individual's personal identity and privacy, and if negligible pecuniary damage results there from.

C. Major specific issues

Video Surveillance

The decision adopted by the Garante on 29 April 2004 referred to the basic principles applying to this subject matter and described the general requirements to be fulfilled by any video surveillance system; guidance was also provided in respect of specific data processing operations – for example concerning the use of video surveillance in schools, hospitals, on board means of transportation, and at the workplace. The Authority reserved the right to take ad-hoc measures in particular situations on a case-by-case basis.

The basic criterion should be respect for citizens' fundamental rights and freedoms and personal dignity, with particular regard to privacy, identity and personal data protection (see Section 2(1) of the data protection Code). Accordingly, the Garante pointed out that individuals may not be deprived of the right to move without interferences that are incompatible with a free democratic society (see Article 8 of the European Human Rights Convention as ratified in Italy by Act no. 848/1955) such as those resulting from invasive, oppressive data acquisitions in respect of an individual's whereabouts and movements – which is being facilitated by the growing system interaction via Internet and Intranets. The Garante also drew inspiration from the guidelines issued by several international and Community fora such as, in particular, the documents drafted by the European data protection authorities within the framework of the Article 29 Working Party and the Council of Europe's guidelines on video surveillance of 20-23 May 2003.

Electoral Propaganda

The Garante clarified that, as a rule, clear-cut information must be provided to data subjects if census data contained in public and/or publicly available databases are used for electoral propaganda. For the purposes of the European and administrative elections scheduled in June 2004, the Garante dispensed candidates and parties making propaganda with the information requirement, which was found to be a disproportionate obligation, if the data were taken exclusively from public lists and the data subjects were not contacted further. No consent was required if the data were taken from lists, registers, documents, and instruments that are held by public bodies and freely accessible pursuant to laws or regulations

(e.g. electoral registers held by municipalities, lists of members of professional rolls, etc.), or if telephone subscriber directories were used to send standard mail messages and/or make direct phone calls. In all other cases, the data subject's prior specific consent was necessary based on an information notice specifying the purposes for which the data will be used.

'Institutional' SMS-Messaging

The Garante highlighted the principles to be complied with by TLC operators and public administrative agencies in sending SMS messages of an 'institutional' nature, i.e. the messages used by central and/or local authorities to wage information and awareness-raising campaigns or else to disseminate publicly relevant information.

In a decision of 7 July 2004 concerning SMS-messages sent by the Italian Government to inform citizens about the voting procedures of the 13 June 2004 European elections, the Garante confirmed the view it had voiced in a decision adopted in March 2003 and recalled that institutional SMS-messaging is lawful only in the case of emergency and exceptional situations. More specifically, it should be distinguished between the messages sent by telephone operators at the request of public administrative agencies and those sent directly by public bodies. In the former case, the subscribers' explicit consent will not be required exclusively if the messages are sent in connection with natural disasters and other emergency situations, further to the adoption by the relevant public body – if so allowed under the law – of an emergency measure for the purposes of public order, public health and hygiene. In the latter case, i.e. when SMS-messages are sent directly by public bodies, no consent will be required in respect of 'institutional' communications as such. However, in both cases the telephone operators and the public bodies concerned, respectively, will have to provide prior, adequate information to users in respect of mechanisms and purposes of the processing performed on the personal data in question, as well as in respect of the possibility of receiving institutional messages.

This same stance was taken following the tsunami events of 26 December 2004, when the Prime Minister's office and the Ministry of Foreign Affairs requested the Garante's co-operation with a view to acquiring, from the relevant mobile telephone companies, data concerning Italian citizens who appeared to be in the areas affected by the tsunami. The request was aimed, in particular, at allowing the Ministry to send an SMS-message urging those users to report their whereabouts.

Telephone Directories

The data protection Code entrusted the Garante with the task of setting out, by an autonomous decision, the mechanisms to enter and use the personal data concerning subscribers (and pre-paid card holders) in publicly available paper and/or electronic directories (see Section 129).

On 15 July 2004, the Garante, therefore, adopted a decision by specifying, in particular, suitable arrangements for data subjects to give their consent with regard both to inclusion of their data into directories and to any further processing of said data for purposes related to commercial or marketing activities, surveys, etc. A specific model form was drafted by the Garante, which all telephone operators subsequently sent to subscribers (January 2005). This form allows subscribers to be informed appropriately

about the purposes for which their data may be included in telephone directories, and to decide whether to consent to what kind of processing (in particular, whether to also consent to receiving commercial information, and how – i.e. by mail and/or by phone – as signified by ad-hoc symbols to be placed beside each entry). It will be unlawful for any entity to send unsolicited communications to a subscriber that has objected to them via the form.

Code of Conduct Applying to the Processing of Personal Data for Statistical and Scientific Purposes

On 16 June 2004 the Garante adopted the code of conduct and professional practice applying to public and private bodies processing personal data for statistical and/or scientific purposes, where they are not included in the National Statistical System (Sistan).

Apart from setting prerequisites and relevant safeguards for the processing of data for statistical and scientific purposes, this code draws an important distinction between market surveys for statistical purposes and market surveys for commercial purposes. The text of the Code was annexed to the consolidated data protection code as required by law. An English version is available at www.garanteprivacy.it

Code of conduct applying to private credit reference agencies

Following a public consultation launched by the Garante, the code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments was finally adopted on 12 November 2004 by all the relevant trade associations with the contribution of several consumer associations. This code will be legally binding since compliance with its rules is a precondition for the processing of personal data to be lawful, and any breach may carry sanctions plus the payment of damages. The main features of the code are as follows:

a) Need for banks and financial companies (i.e. the entities participating in and accessing the credit information systems (CIS) in question) to use a standard, simplified information notice developed jointly with the Garante, setting out the methods used in risk assessment, as well as the mechanisms for data subjects to exercise their rights in practice.

b) Possibility to process only objective, non-sensitive personal data, and prohibition against using hidden codes to categorise customers/applicants.

c) Need to check regularly that the data are accurate, up-to-date, and not excessive, and for keeping data on defaults separate from those coming from public sources. In particular, only data concerning the debtor will have to be processed, and the data subject will be entitled to be informed before his/her data are entered into the system.

d) Need to comply with the retention periods set out in the code, which are the following:
- data on payment defaults that have been remedied may be retained for up to one year or up to two years depending on whether up to two instalments or more than two instalments were at stake, respectively;
- loan applications may be retained for 180 days, whereas they must be erased after 30 days if they are not granted and/or are waived by the applicant;
- data on defaults that have not been remedied may be retained for up to three years as of expiry of the relevant contract/agreement.

e) Only the banks and financial companies participating in the CIS may access the personal data contained therein, and security measures must be adopted to prevent bulk queries.

f) The data extracted from CIS may not be used for the purposes of marketing, surveys or advertising.

g) Managers of CIS are liable to the sanctions (including criminal punishments) set out in the data protection Code in addition to those that can be imposed by the relevant trade associations.

The text of the code was annexed to the consolidated data protection Code as required by law. An English version is available at www.garanteprivacy.it

Public consultation on four key issues: loyalty programmes, interactive TV, RFID and videophones.

In view of the adoption of broad-ranging provisions on the issues in question, the Garante launched a public consultation in December 2004 by calling on user and consumer associations, trade associations, and citizens to give their views on some of the key points to be addressed in developing data protection guidelines for these highly sensitive sectors. In particular, comments and suggestions were sought as for the definition of the categories of data to be collected, purposes of the processing, information notices, obtaining consent, and application of security measures. The deadline for submissions was 31 January 2005.

Outreach

There is a weekly newsletter that has been published since 1999 to provide the public with information on the Garante's activities and also a six-monthly CD-ROM containing a digital archive of the Garante's activities plus the reference legislation, called 'Citizens and the Information Society' (whose twelfth edition was published in 2004). In addition, the Authority continued its training programme (in-house workshops) on the features and/or application issues related to the Data Protection Code as addressed to private and public data controllers.

Reference should also be made to the international conference organised at the Garante's premises on 17 and 18 June 2004, called 'Privacy and Technological Innovations', which provided the opportunity for exchanging views on the issues related to privacy and leading edge technologies. The proceedings were published at the beginning of 2005.

The Authority's website can be visited at www.garanteprivacy.it. Some of the documents are available in English.

Latvia

General information on the Data State Inspectorate

The Data State Inspectorate is a state authority under the supervision of the Ministry of Justice, which began operations in 2001, according to the Personal Data Protection Law. Its duties are determined by Personal Data Protection Law, Electronic Documents Law and Freedom of Information Law. The Data State Inspectorate is acting independently in execution of the functions provided in law and its decisions can only be appealed at the Court.

The Directive 95/46/EC is implemented by the Personal Data Protection Law that came into force on 6 April 2000. Regarding the supervision of personal data protection in Latvia, the Data State Inspectorate has the following duties:

- to ensure compliance of personal data processing with the requirements of Personal Data Protection Law
- to take decisions and review complaints regarding the protection of personal data
- to register personal data processing systems
- to propose and carry out activities aimed at raising the efficiency of personal data protection and submit reports on compliance of personal data processing systems created by government and local government institutions with requirements of regulatory enactments
- together with the Office of the Director General of the State Archives of Latvia, to decide on the transfer of personal data processing systems to the State archives for preservation thereof
- accredit persons wishing to perform system auditing of personal data processing systems of government and local government institutions in accordance with procedure established by the Cabinet of Ministers.

In the field of electronic signature, the Data State Inspectorate carries out the following duties:

- accredits certification service providers in accordance with the voluntary accreditation principles
- checks whether the trusted certification service providers comply with the certification service provision regulations
- monitors that the security of the trusted certification service provider information system and procedures conform to this law, other regulatory enactments and the description of the trusted certification service provider information system, equipment and procedure security
- ensures that the Latvian accredited trusted certification service providers register in which information regarding certification service providers from other states are also included, the issued qualified certificates of which are guaranteed by a Republic of Latvia accredited trusted certification service provider, which is freely accessible in a continuous on-line regime.

Besides all the above mentioned, the Data State Inspectorate supervises the implementation of Freedom of Information Law since 1 January 2004.

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

As has already been mentioned, the Directive 95/46/EC has been implemented by the Personal Data Protection Law that came into force on 6 April 2000. However, in order to comply with the requirement of Article 28 of this Directive, the Data State Inspectorate of Latvia in co-operation with Austrian and German data protection experts have been implementing

the PHARE twinning project No.LV/2002/IB/OT-01 'Data State Inspectorate' (time period for implementation – 15 September 2004 to 15 September 2005). The overall objective of this twinning project is to strengthen the administrative capacity of the Data State Inspectorate to implement data protection acquis, particularly by improving the legal base of the Inspectorate and training the staff. After the implementation of this project, there will be amendments made to the national law so that it will comply with the requirements of Article 28 of the Directive 95/46/EC.

The Directive 2002/58/EC has been implemented into the national legislation by the Electronic Communications Law of 17 November 2004 and the Law on Information Society Services of 4 November 2004.

B. Major case law

No major developments to report.

C. Major specific issues

Staff at the Data State Inspectorate have been participating in several working groups on the national level that concern the data protection issues and which results in different legal acts.

In 2004, major work has been done in order to elaborate a draft Law on Patients' Rights which was forwarded to the Parliament for adoption at the beginning of 2005.

Furthermore, active work has also been done regarding the elaboration of Law on Information Society Services that came into force on 4 November 2004. This law determines the prohibition of unsolicited mail to be sent to a person who has not provided his/her consent for that.

Work has been continued regarding data protection principles to be better implemented in the sectors of social welfare, pharmacy and genetic research.

Lithuania

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

Directive 95/46/EC

The recent amendment of the law (the law was adopted by Seimas on 13 April 2004) concerning prior checking came into force on 24 April 2004. The law narrowed the scope of the prior checking to the processing of sensitive personal data by automated means for the purposes of internal administration or in the cases specified in Article 10 and paragraph 2(6) and (7) of Article 5 of this law; where the data controller intends to process public data files by automated means, unless the laws and other legal acts specify the procedure for disclosure of the data.

Directive 2002/58/EC

- The Law on Electronic Communications entered into force on 1 May 2004 implementing the Directive 2002/58/EC.

- On 22 April 2004, the Code on the Administrative Violations of the Law of the Republic of Lithuania was supplemented by the provisions for the administrative liability for unlawful processing of personal data and violation of the protection of privacy in the electronic communications field. The State Data Protection Inspectorate of the Republic of Lithuania (hereinafter: Inspectorate) supervises how the provisions of chapter IX 'The Processing of Personal Data and Protection of Privacy' of the Law on Electronic Communications are implemented, examines complaints in cases provided by this law in the manner set forth in the Law on Public Administration. The provisions came into force on 1 May 2004.

- On 6 December 2004 the Government of the Republic of Lithuania adopted the Resolution on the rendering authorisations implementing the Law on Electronic Communications.

- On 24 January 2005, the Government of the Republic of Lithuania adopted the Resolution on the amendment of the Regulations of the State Data Protection Inspectorate. In this way, new functions were designated to the Inspectorate according to the Law on Electronic Communications, Europol Convention and the Convention on the use of information technology for customs purposes.

Other legislative developments

- On 22 April 2004, the Seimas of the Republic of Lithuania ratified the Europol Convention. The Law on Ratification of the Europol Convention came into force on 1 May 2004.

On 28 June 2004, the Government of the Republic of Lithuania designated the Inspectorate national supervisory body, the task of which shall be to monitor independently the permissibility of the input, the retrieval and any communication to Europol of personal data and to examine whether this violates the rights of the data subject.

- On 8 March 2004, the Seimas of the Republic of Lithuania ratified the Convention drawn up based on Article K.3 of the Treaty on the European Union, on the use of information technology for customs purposes.

On 15 July 2004, the Government of the Republic of Lithuania designated the Inspectorate responsible for independent supervision of personal data included in the Customs Information System, ensuring that independent supervision and checks are carried

out, and to ensure that the processing and use of data held in the Customs Information System do not violate the rights of the person concerned.

■ The new version of the Law on State Registers was adopted on 15 July 2004 came into force on 7 August 2004.

■ On 19 April 2004, the Government of the Republic of Lithuania adopted the Resolution on the Approval of the Rules on the Establishment and legitimisation of State Information Systems.

■ On 2 June 2004, the Government of the Republic of Lithuania adopted the Resolution on the Order of Compensation for the Disclosure of the Data to the Data Subject and Approval of the Order of Compensation for the Collection of Data from the Registered Data Controllers.

B. Major case law

■ At the beginning of 2004, the parliamentary committee on National Security and Defence informed the Inspectorate about the possible violations of the Law on Legal Protection of Personal Data in the Special Investigation Service.

The Law on Prevention of Corruption establishes the restrictions for the gathering and use of the information about a person seeking or holding a position at a state or municipal institution. The decision to request the Special Investigation Service for information about a person shall be made by the head of an institution or a state politician that intends to appoint or that has appointed the person.

During the inspection it was detected that personal data were provided for persons who were not entitled the right to receive such information. Other violations of personal data processing were detected: Special Investigation Service processed sensitive data without executing prior checking, information was unlawfully collected from some institutions, and the Inspectorate was not notified of cases of automated processing of personal data. The Inspectorate instructed the Special Investigation Service to eliminate the detected violations during the set time. The Special Investigation Service appealed the instruction of the Inspectorate to the Court. The main issue was related to the application of the law especially over concerns regarding the processing of a structured filing system by non-automatic means. The Special Investigation Service contested the Inspectorate's right, established in Article 32 paragraph 1 subparagraph 5 of the Law on Legal Protection of Personal Data, to make recommendations and give instructions to data controllers with regard to personal data processing and protection while the Service was not a data controller. The Court overruled this argument saying that the data controller is a legal or natural person who alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes of the processing of personal data are determined by laws or other legal acts, the data controller and/or the procedure for its appointment may be designated by laws or other legal acts. The processing of data is any operation that is performed upon personal data, such as collection, recording, accumulation, storage, classification, grouping, combination, alteration (supplementing or rectifying), disclosure, making available, use, logical and/or arithmetic operations, retrieval, dissemination, destruction or any other operation or set of operations. The Court found that the Service, by way of

fulfilling its task in preventing the corruption area and processing the personal data, became data controller. There was an argument made by the Service that the Law on Legal Protection of Personal Data is not applicable to the activities of the Service while Article 1 paragraph 5 of the Law states that when personal data are processed for the purposes of State security or defence, this Law shall apply in so far as other laws do not provide otherwise. The Court overruled this saying that there is no reason to allege that the Law on Legal Protection of Personal Data is not applicable. The only absolute exception established in the Law on Legal Protection of Personal Data is that the Inspectorate shall have no right to monitor processing of personal data in courts.

■ At the beginning of May 2004, the adviser of the interim President of the Republic of Lithuania referred to the Inspectorate with the request to examine whether the biggest supermarkets violate the Law on Legal Protection of Personal Data when requesting the personal identity documents and inputting the first seven numbers of customers' identification numbers from it into the cash register.

The Law on Alcohol Control, which came into force on 1 May 2004, provided that it shall be prohibited to sell alcoholic beverages to individuals who are under 18 years of age. Persons who sell alcoholic beverages shall have the right and, if there are any suspicions that the person is younger than 18 years old, are obliged to request, that the individual who is buying alcohol products presents a document attesting his age. If the person does not present a document attesting his age, sellers of alcohol products must refuse to sell him these products. The same provisions on selling tobacco products are in the Law on Tobacco Control.

The supermarkets started to request the personal identity documents from all citizens in order to make sure that alcohol or tobacco products were not sold to customers who were minors.

In May 2004, the Inspectorate carried out checks to see if the requirements of the Law on Legal Protection of Personal Data were being violated while selling alcohol beverages and tobacco products. They found no violations as the supermarkets did not process personal data; one supermarket used the first numbers of a personal identification number for only one purpose – to estimate the age of a person and it was impossible directly or indirectly to identify the person according to them.

■ The Inspectorate received complaints from two persons on processing personal data at the general prosecutor of the Republic, in the secretariat of the Seimas Chairman of the Republic and at the Anticorruption commission (hereinafter: Commission) of the Seimas where the requestors asked to detect whether they legally and legitimately processed the requestors' personal data.

During the time of the investigation, it was established that the Commission, in transferring the copy of notification on suspicion to media representatives, conveyed excessive data relating to the requestors' personal data – personal code, residential address – and did not execute the proper organisational and technical means intended for the protection of personal data against accidental and unlawful disclosure.

For these violations, the chairman of the Commission was issued a protocol on administrative offences, which was subsequently submitted to the Court. The Court cancelled

the case on the grounds of absence of the administrative breach of law.

■ The Inspectorate received a complaint disputing the lawfulness of personal data processing by one joint-stock company (hereinafter: Company X). The requestor claimed that Company X offered a card of benefits which required the provision of a personal code.

During the investigation it was established that Company X presented the blank loyalty card (hereinafter: Blank) to be filled in by a person, who is required to indicate the following data: name, surname, personal code, gender, place of residence, telephone number, electronic mail address. The Company X then processed the personal codes of the clients, although the personal code was not used for any specific purpose; it is not needed for the paying of neither taxes nor any other purpose. It was established that the processing purpose of the data filled in on the Blank is to calculate the number of scores grantable for the persons who fulfil payment (carry out transactions) by loyalty cards at the chain stores web managed by Company X and to disperse the information about the commercial events and promotions carried out in the trading centre to the card owner. But according to the Buyer's card general usage rules, item 4.3 points out that the Company X card owner, presenting the card for the first time and paying for the purchases at Company X stores, will be granted a discount of 10% of the total estimated value of the purchase. Thus the purpose of processing the data filled in on the form is not only a calculation of scores gained and the information related to promotions carried out in the trading process sent to the card owner, but also an application of payoffs for the loyal Company X customers. It was established that Company X customers' personal data had been processed for direct marketing and discount granting purposes. Company X performed processing of one type of excessive personal data – the clients' personal codes.

With regard to Buyers' loyalty cards, adopted by Company X, the general usage rules, item 4.6, say that the card owner by his consent will be informed about topical novelties, promotions and special offers by e-mail, SMS and post. Company X does not introduce the client to the information about his right to object that his personal data might be processed for direct marketing purposes.

For these violations to the Company X director, a protocol of administrative offences was issued. The Court imposed a penalty of 600 Lt. on the Company X director.

■ The Regulations on the State Register of the Personal Data Controllers establishes the requirement for the data controller to designate the person who is in charge of data protection. The data controller indicated in the notification on the processing of personal data that he had designated the person who was in charge of data protection. This information was recorded by the Inspectorate in the Register. During the inspection of the legitimacy of data processing by this data controller, the violations were detected and the protocol on the violation of the administrative law was issued to the head of the company. The company appealed this protocol on the basis that the protocol was issued for an improper subject. The Administrative Court decided that although the laws did not expressly describe the definition 'Personal Data Protection Official', the head of the company had designated a particular person to be in charge of the data protection, and this meant that this person could be considered as a Personal Data Protection Official and, in the case of violation, the protocol for the violation of Administrative Law must be issued to this person.

C. Major specific issues

Personal Identification Number

The Lithuanian system of state registers and information systems processed by the state institutions is based substantially on issuing a Personal Identification Number (PIN) for each resident, which is unique and unchangeable.

The structure of the PIN is described in Article 8 of the Law on the Population Register as well as in clause 18 of the Regulations on the Population Register. Its 11 digits contain information about the date of birth and the sex of the person. According to Article 8 of the Law on Population Register paragraph 2, the structure of the personal number is the following: the first number corresponds to gender and century of birth; second and third – last two numbers of year of birth; fourth and fifth – month of birth; sixth and seventh – day of birth; eighth, ninth and tenth –numbers to differentiate people who were born on the same day; eleventh – control number of the first ten numbers. The personal number is written in personal documents such as a citizen's passport, personal identity card, official passport, driver's licence). The Population Register Service makes and provides personal numbers and prepares the order of provision, which is approved by the Minister of Interior.

The usage of the PIN is restricted according to Article 7 of the Law on Legal Protection of Personal Data. According to Article 7 paragraph 2 of this Law, the use of a personal identification number for the processing of personal data shall be conditional on the consent of the data subject. The personal identification number may be used when processing personal data without the consent of the data subject only if:

- such a right is stipulated in this law and other laws
- for research or statistical purposes in cases specified in Articles 12 (processing of personal data for purposes of scientific research) and 13 (Processing of Personal Data for Statistical Purposes) of this law
- in state registers and information systems provided that they have been officially approved under law
- it is used by legal persons involved in activities related to granting of loans, recovery of debts, insurance or leasing, healthcare and social insurance as well as in the activities of other institutions of social care, educational establishments, research and studies institutions, and when processing classified data in cases provided by law.

Given that the PIN works like a key to quite a lot of further (and partly sensitive) information about the data subject, it has to be very thoroughly evaluated for what purpose the PIN could be used by the data controllers.

In Lithuania, a search can be conducted by only using the PIN, whether in the private sector or in state registers and information systems processed by the state institutions. To change such a search system would require huge financial resources.

It should also be mentioned that the use of the PIN is regulated, not only by the Law on Legal Protection of Personal Data, but also other special laws and secondary legislation regulate its use. In practice, one can find cases where secondary legislation foresees using the PIN although the laws do not provide for such use directly.

In July 2004, the Human Rights Monitoring Institute conducted a research called 'Right to Respect for Private Life: Use of Identity Code in Lithuania'. This research was presented during the meeting of the Chairman of the Seimas and representatives from other governmental and non-governmental institutions concerned with human rights. The conclusion of this research was the following: the structure of identity codes in Lithuania is imperfect. In this country, the identity code discloses personal data (sex, date of birth); in the Lithuanian legal system, a modern standard for protecting the right to privacy in the use of identity codes is not properly adopted as too many subjects can receive the PIN. The massive use of PIN makes its function as an identifier useless because of the legal requirement to indicate it. The PIN of the person becomes easily accessible to the public, making conditions for the misuse of PIN. The Institute recommended: "the rule of 'revelation in the range of authentication' must be inserted into the Law on Legal Protection of Personal Data; the number of requirements to disclose an identity number in other legal acts must be reduced in order to prevent excessive disclosure of personal information; change the structure of the identity code (e.g. to a random sequence of numbers) so it will not reveal any personal information (age, sex) or sharply reduce usage of the identity code by following a principle of adequacy; discard mandatory announcement of identity codes in the media".

The legislation of the Republic of Lithuania on the personal data protection in the state registers was examined by the PHARE project experts. The conclusion was that the legislation on the state registers concerning the data protection complies with the EU acquis, but that the permission for legal persons indicated in Article 7 paragraph 3 subparagraph 4 of the Law on Legal Protection of Personal Data is quite extensive. With respect to the number of legal persons who are allowed to use the PIN, this provision leads less to a restriction but rather to an extension of the use of the PIN.

It is foreseen that the Article 7 the draft Law on Legal Protection of Personal Data will be amended.

State registers

The Inspectorate gave the opinion on the draft Law on State Registers for the Parliament concerning the data protection in the state registers. The biggest issue is the publicity of the data contained in the state registers. The Parliament took into account the opinion of the Inspectorate. The new version of the Law on State Registers was adopted on 15 July 2004 and came into force on 7 August 2004.

PHARE project

At the end of March 2004, the Twinning Project No. LT02/IB-JH-02/-03 Strengthening Administrative and Technical Capacity of Personal Data Protection began at the Inspectorate. One of the main objectives of this project was to raise awareness in society by preparing training packages for the groups of data controllers, those who apply the Law on Legal Protection of Personal Data and issue the decisions (judges, public servants), to prepare the commentaries of the Law on Legal Protection of Personal Data.

The legislation of the Republic of Lithuania on the personal data protection in the state registers was examined by the PHARE project experts. The conclusion was that the legislation on the state registers concerning the data protection complies with the EU acquis, but

that the permission for legal persons indicated in Article 7 paragraph 3 subparagraph 4 of the Law on Legal Protection of Personal Data is quite extensive. With respect to the number of legal persons which are allowed to use the PIN, this provision leads less to a restriction but rather to an extension of the use of the PIN. It has to be taken into consideration to amend Article 3 in the Law on Population Register by indicating the purposes of the Register more precisely. Information about the main purposes as well as the most important recipients of disclosed data has to be made publicly available. A detailed evaluation on which personal data are needed for how long and for what purpose should be made by the population registry. The recipients of multiple disclosures, as well as the explicit conditions, purposes and the extent of data should be indicated in the law.

The extent of data which are stored in the Regulations of Real Property should be checked critically, not only under the aspect of efficiency and customer orientation, but also under the aspect of strict necessity for the legal and economic purposes of the register; the principle of necessity has found expression in the EC Directive and is a main aspect of data protection.

The rules, at least those in the Regulations, should be completed by exact descriptions of the data that are to be registered.

The Regulations could be changed in the following respect: It should be stated that for inquiries there has to exist a legitimate interest and especially in cases of access via internet in every individual case, the user's legitimate interest should be queried and stored for purposes of data protection. Thus, it should be explicitly stated that every research has to be recorded to make it possible to control the legality of the request afterwards. Furthermore, every user should be obliged to use the information only within the scope of the legitimate purposes he submitted. In addition, a general ban on commercial and political use of the data could be stipulated. The disclosure of information should be restricted to the amount that is necessary for the purpose of the register.

Luxembourg

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

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

The coalition programme presented by the newly formed government on 4 August 2004 mentioned their intention to amend the data protection framework law of 2 August 2002 in the view of a clarification and simplification, in particular of the formal requirements and procedures which are not essential for the good protection of the citizens' fundamental freedoms and privacy.

Law of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications

The draft law for the implementation of Directive 2002/58/CE was amended in several points before discussion in Parliament. A mandatory storage and retention period of 12 months was foreseen although the draft specifies that the operators and service providers are permitted to use the data for their own technical, operational and billing purposes for no longer than a maximum period of six months. In respect of telephone and telecommunication directories, the draft only provided for the opt-out principle. The Commission nationale pour la protection des données published its opinion regarding the draft law on 20 February 2004. The law was finally adopted by Parliament on 30 May 2005 and entered into force on 1 July 2005.

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

This law supersedes an old law in respect of the freedom of the press and the liability and obligations of editors and journalists. The provisions concerning exemptions and derogations from the data protection law were finally taken out of the text, as the Parliament decided to discuss the specific rules governing the activities falling under the freedom of expression principles during the adoption of the draft law on data protection.

Law of 6 July 2004 amending the law of 15 February 1955 regarding traffic regulations on public roads

The Commission nationale pour la protection des données issued a critical opinion on some specific provisions of this law, particularly the regulation of the processing of judicial data by a private organisation to which the public authorities have subcontracted certain activities concerning the issuing and revocation of driving licences and the technical control of vehicles. The national DPA had not been consulted before the adoption of this law.

Decrees and secondary legislation

Several decrees were taken in application of the data protection law regarding, among others, the functions of the data protection officials within organisations, personal data processed by certain medical professionals, access of police and urgency services to phone numbers and address data and the processing by the police of personal data for law enforcement purposes.

Other legislative developments

- On 4 March 2004, a draft law was issued for the ratification by Parliament of the Additional Protocol to Convention 108 of the Council of Europe (ETS No. 181) regarding supervisory authorities and trans-border data flows.

- A draft law regarding the use of genetic data for the identification of persons in the domain of law enforcement and criminal law was commented on by the Commission nationale pour la protection des données.

The national DPA made recommendations for improvements regarding an independent supervision of such data processing and of the individual rights granted to the concerned persons.

B. Major case law

There are still no significant court decisions to report regarding the application of the Data Protection law, in civil as well as in criminal matters.

However on 15 December 2004, the Administrative Court rejected the request for cancellation of a decision from the Commission nationale pour la protection des données, forbidding video surveillance of the employees of a shoemaker's store. The Court of Appeal confirmed the decision in July 2005 and ruled out the objections made by the employer on the interpretation of the law by the Commission nationale pour la protection des données and the application of the necessity and proportionality principles.

C. Major specific issues

The Commission nationale pour la protection des données announced in October during a press conference that its activity will focus increasingly on raising awareness amongst the citizens and providing general information to the public.

An information booklet was published in three languages and was widely distributed with the support of the governmental information and press department.

Guidance to data controllers and complaint handling will also get better attention by the national Data Protection Authority. The DPA supports the government's intention to simplify a priori control procedures and notification mechanisms.

The Commission nationale pour la protection des données issued a press release regarding the legal provisions on genetic paternity tests further to a public debate on this topic which received a wide coverage in the media.

Proliferation of video surveillance and surveillance in the employment place, and the use of consumer profiles in new aggressive marketing strategies continue to be the most relevant topics commented by the press.

Malta

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

Directive 95/46/EC was transposed under Chapter 440 of the Laws of Malta by Act XXVI of 2001 as amended by Act XXX1 of 2002 and Act IX of 2003. This Act was brought into force in July 2003, establishing the obligation for notification by July 2004. Certain provisions relating to manual filing systems will be effective from October 2007.

Directive 2002/58/EC was transposed by legal instruments L.N. 16 of 2003 and L.N. 19 of 2003. These were brought into force in July 2003.

Other legislative developments

Before the deadline set for notification, Regulations were published in 2004 (L.N. 162 of 2004) to amend the fees payable and these were reduced to a flat rate of Lm10 (€ 24) per annum; various sectors were exempted from such payment.

Simultaneously, an exercise to simplify notification was carried out and the Notification obligation was no longer required on an annual basis. Only new processes and amendments as they arise are notifiable - and this without payment.

In March 2004, (L.N. 142 of 2004) Regulations were published to make applicable to the police provisions in relation to the processing of personal data for police purposes.

B. Major case law

None to report.

C. Major specific issues

As with the introduction of any new system, there were various teething problems in this implementation stage of the data protection legislation.

Initially data controllers were averse to the payment of high notification fees - this issue was addressed by the revision of the fee structure. Over 8 000 notification forms were received.

Implementation also required the gearing-up of data controllers to their obligations under the new law to match the expectations of the citizens as they gradually grow.

Another issue addressed was the safeguard of minors in relation to information they provide at school, in cases where the children may be the victims of their own parents. Ad hoc regulation was made (L.N. 125 of 2004) to remove the requirement of consent and right of access by such parents when this is not in the best interest of the child.

The Netherlands

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

Directive 95/46/EC was transposed into national law by an act of 6 July 2000[8] and entered into force on 1 September 2001, replacing the old data protection law, the *Wet persoonsregistraties* (Wpr), which dated from 28 December 1988.

Directive 2002/58/EC has been transposed into Dutch law, mainly by modifications introduced in the Telecommunicatiewet (Telecommunications Act), entering into force on 19 May 2004[9]. Other legislation transposing parts of this Directive are, amongst others, the *Wet op de Economische Delicten* (Act on Economic Offences) that implements Article 13(4) of Directive 2002/58/EC.

Combating terrorism

The bombings in Madrid and the murder of Theo van Gogh have resulted in an intensification of the pursuit of a secure society, particularly in the fight against terrorism. In short order, a number of extensions to the powers of the police and the Ministry of Justice were implemented or announced, which will result in more and more information on citizens who are not suspects ending up in police files. For years there have been calls for extended powers, but the increased threat of terrorism since 11 September 2001 has made way for a conviction that such an extension is in fact necessary.

Needless to say, the Dutch DPA (Dutch Data Protection Authority) supports the need for the Government to take effective measures to combat terrorism. However, international treaties, European rules, the Dutch Constitution and other laws demand that new powers meet the joint criterion of necessity and proportionality. Legal protection must also be provided for. It may be necessary to venture out in different directions in the battle against terrorism, but there is no reason to give up the view that the exercise of power and law enforcement must take place within a system of checks and balances: no powers without demonstrable necessity and proportionality and no powers without the use of these powers being monitored.

In their 'terrorism' memorandum to the Lower House on 10 September 2004, the Minister of Justice and the Minister of the Interior and Kingdom Relations announced new methods and powers aimed at combating terrorism. Among other things, the Government envisaged comprehensive collection, linking and analysis of information about groups and persons as the key to preventing terrorism. For this purpose, the Government deemed it necessary to extend competences in the area of detection powers. It announced it would change the scope of application of the legal criterion – 'suspicion or reasonable suspicion of involvement' – for the authorisation of such actions as tapping telephones, monitoring Internet use and surveillance to 'indications of involvement'. The information exchange between security services, the police, the Public Prosecution Service and the IND (Immigration and Nationalisation Service) was to be intensified by means of an information hub, the counter-terrorism info box, where files would be combined and analysed.

[8] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Staatsblad 2000 302. An unofficial translation of the act is available at the website of the Dutch Data Protection Authority, www.dutchDPA.nl or www.cbpweb.nl.

[9] Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), Staatsblad 2004, 189.

According to the Ministers' memorandum, for the Government the mere fact that a citizen acts suspiciously is sufficient reason to put him under surveillance to assess whether the suspicion is justified or not.

In a public response to the proposals, the Dutch DPA came to the conclusion that the necessity to extend powers to collect information had not been demonstrated. The new powers would be an addition to the anti-terrorism legislation that came into effect on 1 September 2004. The scope of the Criminal Code was expanded with new penalisations and through increasing the sentences for criminal offences with terrorist objectives. Conspiracy (in other words 'making arrangements') to commit terrorist acts also became a criminal offence. No experience has yet been gained with these new legal stipulations for information processing that provides an insight into the necessity and proportionality of the proposed measures. Added to this there are the recently implemented or yet to be implemented powers to intercept telecommunications and the power to request information from companies and other organisations.

Furthermore, the proposed far-reaching coordination of the gathering of information fails to recognise the separate legal responsibilities and powers of intelligence services and the police. Protecting the security of the state is primarily the business of the intelligence services. These services have far-reaching powers to collect information at the merest hint of suspicion that the security of the state is at risk. The police can only receive information from the General Intelligence and Security Service if this aids them in their performance of police duties. The Dutch DPA therefore issued a warning against a development whereby information on many citizens who are not suspects would end up in police files.

The proposed plans also lacked a proposal for the adequate and structural control of the process of collecting and sharing information. It would be a serious shortcoming if the Government did not provide for such a control. A lot of information shared would remain hidden, also to persons who were the unjustified subject of an investigation. It is therefore all the more necessary to build in controls for the exertion of these far-reaching Government powers. Citizens must be protected against terrorism, but must also be able to have confidence that the Government will exercise its far-reaching powers legitimately.

Duty of identification

Early in 2004, the Dutch DPA advised the Minister of Justice against submitting the legislative proposal to widen the scope of citizens' duty to identify themselves. The main argument for this advice was that the legislative proposal created a general duty for citizens to identify themselves, both to the police and to other supervisory authorities. However, the legislator did not sufficiently substantiate and justify such a general duty.

Only a few years ago the Government concluded that a general duty for citizens to identify themselves was too far reaching. The explanatory memorandum which accompanied the legislative proposal did not raise any new arguments and the Government therefore failed to meet the requirement in Article 8 paragraph 2 of the ECHR, which stipulates that interference with the right to privacy must be sufficiently justified. Neither were the possible discriminatory and stigmatising effects of the proposal acknowledged. On 1 January the extended and de facto general duty for citizens to identify themselves came into force.

New police information system

In recent years, the different police forces have developed a colourful range of ICT applications to perform the same tasks. Eventually the decision was made to try to achieve nationwide uniformity in the area of ICT. As the supervisory authority for the processing of data by the police, the Dutch DPA was asked to advise regarding the statutory rules that affect the choice of new systems.

In addition, work also commenced on the revision of the statutory framework for a police information system. In 2004, the Minister of Justice received advice regarding the draft legislative proposal on the Police Data Act. The Dutch DPA agrees with a system for processing police data in which the guarantees increase as the processing constitutes a greater risk for the data subjects involved. There were also three important areas of criticism. Firstly, more emphasis is needed on the quality of data processed by the police. Secondly, the Dutch DPA seriously objects to the introduction of so-called theme files: large collections of data about citizens who are not suspected of anything. Thirdly, clear rules are required in respect of retention periods. Data that is no longer required should be destroyed rather than retained indefinitely 'just in case' the information might be needed in future.

Health Insurance Act

The new Health Insurance Act provides for a mandatory standard of health insurance for all residents. In 2004, the Dutch DPA advised that, in respect of the legislative proposal, more concrete standards should be set for the use and exchange of personal data in the context of health insurance. The structural supervision of health insurance companies would otherwise mainly be limited to highlighting unlawful situations in insurance-related, financial and administrative areas. Supervision of the processing of personal data must also be specifically included in the legislative proposal because the processing of personal data by the health insurance companies also requires structural supervision. In addition, the draft addendum of the Association of Dutch Health Insurers (ZN) with the Code of Conduct for the Processing of Personal Data for financial institutions must be adjusted.

The new Occupational Disability Insurance Act and insurance companies

In respect of the new occupational disability insurance system, the Dutch DPA advocated greater clarity about the positions the various parties (employer, employee, UWV [employed persons' insurance administration agency], reintegration agencies and insurance companies) take up in relation to each other when it comes to the use of personal data. The way in which insurance companies will deal with personal data in the new system is unclear, and this is not a desirable situation.

As a result of the new tasks pursuant to the Work and Income based on Employment Capacity Act but also, for instance, the new Health Insurance Act, the corporate groups, of which the insurance companies are a part, will have access to even more (medical) personal data. This creates the potential for a powerful and influential information position.

Insurance companies do, however, acknowledge the importance of the careful processing of personal data. If the Government fails to establish rules for this type of processing it will be time-consuming and inefficient for the parties involved in the processing. The Dutch DPA has therefore urgently advocated to the Minister of Social Affairs and Employment that clarity must

be provided in the relevant legislation regarding the possibilities and limitations relating to the processing of personal data.

B. Major case law

Compliance with the notification obligation

Pursuant to the Personal Data Protection Act (WBP), companies, organisations and institutions are obliged to notify the processing of personal data to the Dutch DPA or their Data Protection Officer, unless there is an exemption. If data processing has been notified incorrectly or incompletely, or has not been notified at all, the Dutch DPA can impose a penalty to a maximum of € 4 500. Notifications from certain sectors or regarding certain types of processing are periodically subjected to a further investigation. The Dutch DPA also carries out such investigations as a result of complaints from data subjects.

In 2004, the annual investigation focused on three sectors, namely telecommunications, mental healthcare and debt collection. The investigations will be finalised in 2005 and sanctions may or may not be imposed.

As a follow-up to specific information provided to the telecom sector, the Dutch DPA checked whether a number of providers of telecommunications services (fixed and mobile telephony and Internet) complied with the notification obligation. This investigation focused specifically on the notification of the processing of telecommunication traffic data.

In a number of Area Health Authorities (GGDs), the Dutch DPA investigated the notification of the processing of personal data in the context of the Public Mental Healthcare (OGGZ). It is the legislator's opinion that this processing carries specific risks for the privacy of the citizens involved; when notifying the Dutch DPA of the processing the data controller must therefore also request an investigation into the lawfulness of the processing, the so-called preliminary investigation.

Analysis of the WBP notifications register showed that the number of notifications by debt collection agencies lags behind considerably. Supervision in this sector was aimed at investigating to what extent debt collection agencies process personal data and to what extent their failure to notify the processing of personal data was correct.

Penalties for municipalities and companies

In 2003, the Dutch DPA performed the first random check on the compliance with the WBP notification obligation among a number of municipalities, health insurance companies, internal and external occupational health and safety services (arbodiensten) and direct marketing companies. The number of WBP notifications increased greatly after these initial checks, not only in the investigated sectors but also among the private detective agencies, the police and in the healthcare sector.

A total of 50 investigations were carried out in the context of this initial check. In a number of cases, a supplementary check was carried out on site in order to establish the facts. At the end of 2003, the random check resulted in the first penalties for a municipality and two companies.

In the course of 2004, the DPA imposed a total of 29 penalties ranging from € 3 000 to € 15 000. In a number of cases, the Dutch DPA used its authority to reduce the penalty, especially if, as in the case of municipalities, there was a high level of processing of personal data. The main consideration was that even a reduced penalty would achieve its objective, namely a special and general preventative effect.

The aforementioned penalties were imposed on 14 municipalities, three direct marketing companies, three health insurance companies and nine occupational health and safety services. Most municipalities submitted an objection against the penalty; a number of municipalities have now paid the penalty. None of the private organisations except one submitted an objection and nearly all have now paid. All the organisations involved have now notified the Dutch DPA of their processing of personal data.

Criminal investigation units

In 2003 and 2004, the Dutch DPA carried out investigations into special police registers held by the criminal investigation units (CIE) of the regional police forces. Pursuant to the Police Files Act (Wpolr), the Dutch DPA is the regulator supervising the use of the police files. In this position the Dutch DPA has access to the content of the CIE files. Because of their sensitive nature these files are, quite rightly, largely protected from access by the registered persons involved and from supervision by the Court. In this context the Dutch DPA considers it a special responsibility to supervise the CIE files substantively.

In its investigations, the Dutch DPA focused mainly on checks based on the content of the files, and a number of technical and organisational aspects were also taken into consideration. The general picture emerging from the investigation is mostly positive. The substantive aspects that were investigated generally proved to be in order. With regard to the investigated technical and organisational aspects it became clear that on a number of points the rules imposed by legislation and regulations are not being met. The police forces have indicated that, whilst awaiting an information system to be implemented on a national basis, they will not make any adjustments to the current systems and methods.

National registers in the healthcare sector

In 2004, the Dutch DPA completed its investigation into the operation of national registers in the healthcare sector with a report that was published in April 2005. The key questions of the exploratory investigation were what does the patient know about the registration of his data in national data banks, for what exact purposes are these registers used and can the information in these registers be traced back to the individual patients? In view of the sensitivity of the information and the professional secrecy that applies to physicians, the law currently only offers limited possibilities for the processing of (indirectly) traceable patient data.

The investigation of five national registers gave the Dutch DPA the impression that the investigated national registers generally handle the personal data reasonably well. It also emerged that, in nearly all cases, improvements were possible and necessary. The main measure to be implemented is limiting the traceability of the data to individual patients. A number of recommendations have now been adopted by the registers.

C. Major specific issues

Cameras in the public domain

The interest in video surveillance has only increased in recent years. The general public also accepts cameras, expecting video surveillance to be effective. Video surveillance, particularly on the part of the Government, has increased considerably in recent years. This is why, in 2003, the Dutch DPA initiated a study into the nature and scope of video surveillance by Dutch municipalities. Among other things this study showed that 20% of municipalities use video

cameras and that in many of these municipalities the effectiveness of the video surveillance had not (yet) been evaluated. Subsequently, a study entitled 'Cameras in the public domain' was published in November 2004 with rules of thumb for decision-making, starting points for the placement and use of cameras, the rights of data subjects, monitoring and evaluation.

Citizens Service Number

The policy for an 'electronic Government', a government that makes optimum use of information technology, including the Internet, was outlined in 2004 in the programme entitled 'A different Government'. The introduction of the Citizens Service Number (BSN) is an absolute condition for the success of this programme. The BSN programme agency was established with the instruction to implement the plan that was finalised at the end of 2003.

The Government unexpectedly made the decision – contrary to its earlier promises – to introduce the BSN in the healthcare sector as well. Healthcare institutions and health insurance companies will be obliged to use this number. The use of a unique personal identification number in the healthcare sector has inherent risks; large-scale linking of (patient) data becomes easier and, therefore, so does abuse. However, a separate care identification number – a safeguard against the too-easy distribution of information on patients and healthcare recipients – no longer proved feasible in the political and social arena. The Dutch DPA subsequently approved the use of the BSN in the healthcare sector, provided it was accompanied with compensatory guarantees, including reliable authorisation procedures for the use of medical data that becomes accessible with the number.

In 2005, the so-called *Nationale Vertrouwensfunctie* (National Trust Function) was prepared, in which the Dutch DPA plays a part. This is an organisation that provides for structural monitoring in the form of, among others, an office where citizens can take their questions and complaints about the BSN.

Codes of Conduct

In 2004 it was possible to approve five sectoral codes of conduct. After a preparatory process spanning many years, in which the Dutch DPA tried to support the sector association, the code of conduct for private investigation agencies was approved early in 2004.

The Royal Professional Association of Court Bailiffs developed a code of conduct comprising rules for the special situation whereby court bailiffs act as public functionaries and also provide commercial services (for instance debt collection). It is essential that they do not use the information obtained pursuant to their special legal status as a civil servant in the performance of their non-public activities.

The sector organisation for Recruitment, Search and Selection (OAWS) revised and updated its code of conduct that indicates for which purposes personal data of potential candidates can be processed. The 'Good Behaviour Code of Conduct', a code of conduct for health research, was also revised and rules for the processing of patient data in health research have been incorporated. New is the code of conduct for the processing of personal data in research and statistics, which was formulated by three organisations: the Association for Policy Research, the Association for Statistics and Research and a professional association for market and policy researchers (www.MarktOnderzoekAssociatie.nl).

In 2004, *Zorgverzekeraars Nederland*, the sector association for health insurance companies, started on the formulation of rules of conduct for, among other things, the use of the large quantities of medical data that health insurance companies receive in the context of healthcare claims. Rules will also be formulated for the investigation of fraud committed by an institution, care provider or insurant. This concerns an addition to the Code of Conduct for the Processing of Personal Data of the financial institutions. Expectations are that these rules of conduct can be furnished with an approval at the end of 2005.

Work and Assistance Act

For the purpose of monitoring compliance with the new Work and Assistance Act, in 2004, the IWI (Work and Income Inspectorate) and the Dutch DPA have expressed their intention to enter into a collaboration agreement. This was realised in 20005. Through collaboration and the sharing of knowledge, a more effective and efficient supervision will be possible. Collaboration also promotes unambiguous supervision because the standards used by the regulators can be coordinated. This can also lessen the regulatory pressure for organisations under supervision. For example, the agreement will stipulate arrangements in respect of sharing supervisory information and the mutual provision of information regarding the results of investigations.

Spam

Unsolicited e-mails sent in large quantities, better known as spam, are a nuisance, are difficult to eliminate and incur high costs for Internet service providers, and therefore for their customers. According to recent estimates approximately three quarters of all e-mails sent worldwide are spam. The European Directive on Electronic Communications (2002/58) prohibits the sending of unsolicited commercial messages and the European regulators supervising compliance with this prohibition work together in the so-called Contact Network of Spam Authorities to exchange information and facilitate collaboration in the enforcement of the prohibition in the EU. A collaboration agreement has also been formulated for this purpose.

In the Netherlands, the OPTA (Independent Post and Telecommunications Authority) and the Dutch DPA signed, on 19 October 2004, agreements regarding collaboration in respect of the prohibition on spam, which in the Netherlands has been in force since 19 May 2004. The Dutch DPA will focus primarily on supervising the collection and use of e-mail addresses. Individual complaints regarding spam can be addressed to the OPTA via www.spamklacht.nl. The practical agreements about dealing with spam constituted the prelude toward a broader collaboration protocol between the two authorities signed in July 2005.

Private Investigation

In 2004, a special supervisory arrangement was created for the private investigation sector. The Act for Private Security Organisations and Detective Agencies does standardise the sector, but rules for the realisation of investigations and the further processing of the data collected in such investigations were lacking. The scope of the code of conduct of the Association of Private Security Organisations, which provides for this, was expanded because the Minister of Justice made this code of conduct mandatory for all private investigation agencies by Ministerial decree. The Dutch DPA and the Minister of Justice have entered into co-operation for the monitoring of compliance with this code of conduct.

Poland

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

In the beginning of 2004, works on the amendment of the Act on the Protection of Personal Data came to an end. These regulations entered into force on 1 May 2004, that is, at the moment of Polish accession to the European Union. The activities aimed at amending the provisions, which resulted from the need to fully adapt the Act to the requirements of the 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 the free movement of such data, (hereinafter: Directive), as well as the need to modify some provisions which caused problems in their practical application.

The most important amendments introduced as a result of the amendment of the Act on Personal Data Protection, adapting its provisions to the Directive, include:

- resolving clearly the way that the Act shall also apply to the situation in which personal data is or can be processed outside from the computer filing system
- ensuring free movement of the data between the Member States of the European Union, and the states outside it, which are the members of EEA, by assuming that the conditions of personal data transfer outside the territory of Poland specified in chapter 7 of the Act can apply only to the transfer of personal data to a third country, that is the country that is not a member of European Economic Area
- limiting the subjective scope of application of the Act by excluding from its requirements the subjects established in or residing in a third country, using technical devices located in the territory of Poland for data transfer only
- limiting the application of the provisions of the Act if the processing is related to press journalistic activity, literary or artistic activity, except for situation where the freedom of expression and information dissemination considerably violates the rights and freedoms of the data subject
- introducing the obligation for data controllers established in or residing in the third country who process data in the territory of the Republic of Poland to appoint their representative in the Republic of Poland
- introducing a so-called prior check of data processing accuracy, according to which the controllers of sensitive data, referred to in Article 27 paragraph 1 of the Act may start their processing in a data filing system only after having registered the filing system, unless the controller is exempted from the obligation to notify a filing system to the registration by virtue of the Act.

Moreover, as a result of the amendment, the Inspector General was entitled to issue, in case of any breach of the provisions on personal data protection, decisions ordering to restore the proper legal state, not only in relation to the subject being data controller, but also to all subjects processing personal data. The scope of information available in the open register of personal data filing systems run by the Inspector General was limited (for example there is no information concerned technical and organisational security measures), but the issue relating to the procedure of notifying the changes to information included in the notification of data filing system to registration was regulated.

As a result of the amendments introduced to the Act on the Protection of Personal Data, the following enforcement law provisions were

introduced as of 1 May 2004:

- Regulation of 29 April 2004 by the Minister of Internal Affairs and Administration as regards specimen for the notification of a data filing system to the registration by the Inspector General for Personal Data Protection (Journal of Laws No. 100, item 1025)
- Regulation of 22 April 2004 by the Minister of Internal Affairs and Administration as regards specimen of personal authorisation and service identity cards of the inspectors employed in the Bureau of Inspector General for Personal Data Protection (Journal of Laws No. 94, item 923)
- Regulation of 29 April 2004 by the Minister of Internal Affairs and Administration as regards personal data processing documentation and technical and organisational conditions, which should be fulfilled by devices used for personal data processing (Journal of Laws No. 100, item 1024).

The latter of the above-mentioned regulations introduced specific security levels of personal data processing within the computer systems.

At least the basic security level shall be applied if sensitive data (Article 27 of the Act) are not being processed within the computer system, and none of the computer system devices used for personal data processing is connected to the public network.

At least medium security level shall be applied if data referred to in Article 27 is processed within the computer system and none of computer system devices used for personal data processing is connected to the public network.

High security level shall be applied if at least one of the computer system devices used for personal data processing is connected to the public network.

On 16 July 2004, the new Act on Telecommunication Law was introduced (Journal of Laws No. 171, item 1800), and it came into force on 3 September. The Act was aimed to implement fully, among others, the requirements of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the privacy in the sector of electronic communications into the Polish legal order.

In 2004, the works aimed at ratification by the Republic of Poland of the additional protocol to the Convention No. 108 of the Council of Europe have started. The ratification by the President of the Republic of Poland is expected to take place in 2005.

B. Major case law

On 13 July 2004, the Constitutional Tribunal stated the discrepancy between the Constitution and some regulations of the Act of 23 November 2002 on the amendment of the Act on communal self-government, and on the amendment of some other acts concerning the anticorruption regulations. The Act imposed an obligation on councillors and the people performing functions in executive bodies of territorial self-government units (deputy Major, treasurers and directors of organisational units of self-government) to lodge a written declaration concerning economic activity conducted by the spouse, descendents, ascendants and brothers and sisters. This declaration is public.

In view of the Constitutional Tribunal, the disclosure of information about descendants, ascendants and brothers and sisters is not indispensable for proper functioning of the democratic state of law. This means a breach of constitutional principle of proportionality (Article 31 of the Constitution of the Republic of Poland)

in reference to the principle of the democratic state of law (Article 2). Moreover, the public announcement of the information required by the questioned Act can violate the privacy of persons who are not performing any public functions (Article 47 of the Constitution).

The Constitutional Tribunal has separately treated the spouses of the officers of the territorial self-government units, because staying in cohabitation (and often in joint property of husband and wife) causes the situation in which any income obtained by any of the spouses can be an income for the officer of territorial self-government. Because of the lack of motion from the Commissioner for Civil Rights Protection, the Constitutional Tribunal did not issue any opinion concerning the problem of public access to the mentioned property declarations.

On 25 August 2004, the Provincial Administrative Court in Warsaw dismissed the decision of the Inspector General ordering the erasure of the personal data of the debtor, stored in the Credit Information Agency (BIK S.A.) after the termination of the contract. Banks and the Credit Information Agency justified the practice of maintaining the data of the debtors after the full payment of their obligation, by obligatory, aside from the contract, regulations concerning data gathering and making data publicly available by the Agency. According to these regulations, the Agency is obliged to process the data sent by the bank for five years (from the day of the closure of an account, if the account did not show any arrears above 30 days), or seven years (from the day of the closure of an account, if the account did show the arrears above 30 days). The Court agreed with the opinion of the Inspector General that the regulations do not contain the obligatory law, and cannot be a source of the rights and obligations for bank clients.

In the jurisdiction of the Supreme Administrative Court there was a case concerning the scope of personal data which can be processed by the banks, in relation to the credit agreement. In the context of this case the Supreme Administrative Court issued an opinion on the admissibility of determination by the Inspector General about the proportionality of the scope of data gathered by banks. On 13 July 2004, the Supreme Administrative Court pronounced a judgement in connection with an appeal by the Inspector General on the earlier judgement issued by a different bench of the same Court on the decision by the Inspector General ordering the bank to stop processing personal data acquired by making copies of identity cards in order to get information on the description of appearance, names, outdated place of residence, children and other people who are taken care of by the data subject, or an erasure of personal data of the debtors register.

The Supreme Administrative Court by dismissing the last resort appeal by the Inspector General upheld the argumentation presented by the First Instance Court according to which it is unacceptable for the data protection authority to substitute the legislator in constructing the catalogue of personal data possible to be processed when credit agreement is concluded. In other words, if there is no specific regulation concerning the scope of personal data, the data protection authority cannot determine if the data is adequate.

C. Major specific issues

By the Act of 1 April 2004, on the amendment of the Act – Banking Law, Article 112b has been added to the provisions of the Act on Banking Law, which authorises the banks to obtain

personal data from identity cards by copying these documents.

The action of the banks copying the documents in order to confirm an identity of a client was questioned in the proceedings conducted by the Inspector General because of the lack of legal basis for such kind of practice. Currently, according to the provisions Implemented by the Act on amendment of the Act – Banking Law – banks can process data obtained from identity cards of natural persons for conducting their banking activities only. Acquisition of data from those documents by the banks is acceptable on the ground of the Act on the Protection of Personal Data, which is one of the prerequisites of personal data processing (Article 23 paragraph 1 and 2).

In 2004, the Inspector General repeatedly worked on the problem of making personal data of debtors available for vindication companies, based on the transfer of a claim. Very often the vindication companies to which claims were transferred operated on the borderline of the law, by intimidating the debtors, or freely changing the costs of proceedings.

From the point of view of the Act on Protection of Personal Data, the legality of personal data processing by vindication companies is of paramount importance.

The transfer of claim was regulated by Article 509 and following the Act of 23 April 1964, Civil Code (Journal of Laws Nr. 16, item 93). In this case the provisions concerning the protection of consumers' rights can also be used, in the scope of application of the so-called abusive clause. According to Article 385 paragraph 5 of the Civil Code, it is prohibited for the contracting party to transfer rights and duties of a consumer without his/her consent. The President of the Consumer and Competition Protection Office took the position according to which, with taking into consideration the actual reality of commercial traffic, the practice of transferring the claim to vindication companies "diminishes guarantees and rights of the consumers".

Consequently, considering the above, the Inspector General often presented a point of view that in the case of persons being consumers, making their data available in connection with the transfer of a claim is possible only with the consent of a data subject. In this case, none of the remaining prerequisites of legality stated in Article 23 paragraph 1 of the Act on the Protection of Personal Data can be used.

The cases concerning personal data processing in connection with the transfer of claim were the subject of proceedings of the Voivodeship Administrative Court in Warsaw, as well as the Supreme Administrative Court. It needs to be underlined that such cases cause a lot of controversy in the jurisdiction of Administrative Courts.

In 2004 – and in previous years – the Inspector General considered many complaints concerning direct marketing firms. Those institutions had a problem with proving the legality of data processing, or with meeting an obligation of informing the subjects about the processing of their personal data. This year many controllers tried to avoid the Polish provisions on personal data processing by transferring (at least formally) the process of data processing to other countries (the United States or Cyprus). In those cases, because of limited access to direct marketing companies, the Inspector General notified the prosecution bodies of a crime.

Portugal

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

Law 43/2004 of 18 August provided for specific rules for the organisation and functioning of the DPA. It provided an autonomous framework for the staff and opened the possibility for the DPA to charge a fee for notification and to sell publications and forms. The independent statute of the members/Commissioners and the administrative autonomy remains unaltered.

Directive 2002/58/EC was transposed into national law, through two different legal instruments:

- Decree-Law 7/2004 of 7 January, which transposed the E-Commerce Directive and Article 13 of Electronic Communications Directive
- Law 41/2004 of 18 August, which transposed the Directive.

Decree-Law 35/2004 of 21 February is about the use of video surveillance for the protection of people and goods. This provides a legal ground for the DPA to authorise the use of video surveillance for this purpose, in spite of having the need to make an evaluation on a case-by-case basis, in particular concerning the proportionality principle.

Law 35/2004 of 29 July regulates the Labour Code. It states that any personal data processing through biometrics technology or video surveillance at the work place must have a prior opinion of the workers council.

B. Major case law

The DPA decisions can be appealed to the Administrative Court or to the Criminal Court of summary jurisdiction, in case there are sanctions involved. During 2004, there were four judicial decisions concerning the application of fines. Three of them kept the decision of the DPA and one lowered the sanction from a fine to a warning.

One interesting case regarded the communication from a telecommunications service provider of its clients' data, without their consent, for a third party, which has made consumer profiles and used them for marketing purposes.

Another case concerned a website that published a list with names and photos of alleged debtors and bound cheques.

C. Major specific issues

RFID

The Portuguese DPA issued a recommendation concerning the processing of personal data through radiofrequency identification (RFID). The DPA considered that whenever the use of RFID technology implies the interconnection with personal information then that means that there is a personal data processing. Subsequently, that data processing has to be notified to the DPA, the data have to be collected for explicit and legitimate purposes and cannot be interconnected for other purposes. The data shall be adequate, pertinent and not excessive, and collected in a transparent way, providing the data subject the right to information. The data controller has to post warnings on the products and in the locality where RFID technology is used. Whenever there is remote activation/reading the data subject has to be informed when that will occur. Personal data have to be deleted as soon as they are no longer pertinent for the purpose, as well as any interconnection established in the meantime. This document can be found in Portuguese on our website at: http://www.cnpd.pt/bin/decisoes/2004/htm/del/del009-04.htm

Biometric data

The Portuguese DPA issued some guidelines regarding the use of biometric data at the workplace for the purposes of controlling access and assiduity. There is an English version of the document on our website at: http://www.cnpd.pt/english/bin/guidelines/guidelines.htm

Video surveillance

The DPA set general principles applicable to the use of video surveillance, taking into account the renewed legal framework on this matter. Legitimacy, ways to exercise the right of access, communication to law enforcement authorities were dealt in this document. It can be consulted in Portuguese at: http://www.cnpd.pt/bin/orientacoes/principiosvideo.htm

The DPA also dealt with a specific case regarding the use of video surveillance in kindergartens, in almost every room, allowing the parents to follow on the Internet the daily life of all the children through a password of access. The DPA forbade this data processing for being disproportionate, for compromising the children's rights to privacy and for being abusive to the workers, who would be constantly observed.

Audit to hospitals

During 2004, the Portuguese DPA carried out an exhaustive audit of all departments in 38 hospitals, both public and private. The general aim was to obtain an overview of how health data was being processed and if the rights of the data subjects were being respected. Internal procedures for information circulation within the hospitals, levels of access to information, the analysis requests and collection of information; the access to the patient unique file, telemedicine experiences, video surveillance were the major topics audited. The DPA elaborated an audit report, with specific conclusions and recommendations, which was sent to the hospitals involved, to the Parliament, to Government and to the professional associations concerned. The report can be consulted on our website in Portuguese at: http://www.cnpd.pt/bin/relatorios/outros/Relatorio_final.pdf

Euro 2004

The DPA performed a very active role, following closely the organisation of the European Championship. There was much data processing involved, which was duly registered and authorised by the DPA. The organisation of the Euro 2004 reported periodically to the DPA.

E-vote

The DPA authorised and followed up in loco the first pilot experience regarding e-voting in the elections to the European Parliament. It was a non-binding in-person voting, which was carried out in nine different places. After casting the vote the traditional way, a person could voluntarily try the electronic way.

Slovakia

Slovakia became a Member State of the European Union on 1 May 2004 and a new official name was given to the Office for Personal Data Protection (by the Act No. 428/2002 Coll. on personal data protection as amended, effective as of 1 May 2005). It is now called the Office for Personal Data Protection of Slovakia.

Mr Gyula Veszelei is President of the Office for Personal Data Protection of Slovakia.

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

Implementation of Directive 95/46/EC

In line with the plan of the Slovak Government's legislative tasks for 2004, the Office for Personal Data Protection has prepared a draft law, which amended and supplemented the Act No. 428/2002 Coll. on Personal Data Protection. In September 2004, the Slovak Cabinet passed the Resolution of the Slovak Cabinet No. 895 at the 101st session and thus approved the draft law. The draft law was submitted to the Slovak National Council on 30 September 2004 and was passed on 3 February 2005. The President of Slovakia signed the Act on 28 February 2005 and it was published in the Collection of Acts as Act No. 90/2005 Coll. with effect as of 1 May 2005 (hereinafter: Euro amendment).

The aim of this Euro amendment was to meet the content of the evaluating report elaborated by the European Commission in November 2003. The comprehensive monitoring report on Slovakia's preparations for membership, which required full harmonisation of the Act on Personal Data Protection with the European Parliament and Council's 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 (hereinafter: Directive 95/46/EC). A clear request resulted from the evaluating report so that Slovakia would, without undue delay, meet the requirement of the European Commission so that its supervision body in the field of personal data protection will have investigation and intervention rights and will carry out its functions fully independently, not just from executive power but also from any other state authorities. The independence was also expected in the financial area and personnel policy, which should be subordinated exclusively to the chairman of the office.

The Euro amendment also reacted to the comments raised by the European Commission.

The main principles of approved amendment were:

- specification of some concepts and implementation of new concepts corresponding with the content of Directive 95/46/EC
- application of the articles of Convention 108 and recommendations of the European Council released for personal data protection area
- specifying and making clear the controllers' basic obligations
- restriction of registration of information systems in the context of reinforcing the position of a responsible person delegated in written form in accordance with the Directive 95/46/EC
- introduction of special registration for some risky processing operations in line with Directive 95/46/EC
- specifying the process of procedure and admission of notifications of natural persons
- specification of provisions related to the cross-border transmission of personal data into third countries and transmission of personal data within EU Member States.

Draft amendment to the Act, which was submitted for interdepartmental review, respected the last evaluating report of the European Commission of November 2003. Also in that part was the fact that Slovakia should meet the request of the European Commission so that the supervisory authority in the field of personal data protection, the Office, would have the right to execute its functions fully independently not just from the executive power, but also from any other state authorities. The independence was also expected when financing the activities of the Office and personnel policy, which should be subordinated exclusively to the chairman of the Office. Article 1 paragraph 3 of the Supplementary Protocol to Convention 108 obliges the parties of the convention to provide the supervisory authorities with the personal data protection in individual states with such a position, quoting: "Supervisory authorities execute their functions fully independently." The same requirement results from Article 28 paragraph 1 of the Directive 95/46/EC.

The fully independent position of the Office, which is participating in the protection of basic rights and freedoms of individuals (personal bodies) while processing their personal data and protection of their privacy, can be ensured in line with the constitutional order of Slovakia, just created in the Slovak Constitution. Therefore, it is inevitable to classify the Office among those authorities, which have independence recognised by the Slovak Constitution. In connection with the mentioned requirements of the European Commission, the Office prepared and submitted the requirement in a form of legislative draft law to the chairman of the Slovak National Council in January 2004. This draft law assumed creating the Office as an individual state authority in the Slovak Constitution. The Office stopped to uphold this bill since the amendment draft to the Slovak Constitution was rejected.

The Act No. 576/2004 Coll. on Healthcare, Services Related to Healthcare Provision and on Amendment and Supplement to Certain Acts caused so-called indirect amendment to the Act on Personal Data Protection.

The Act became effective on 1 January 2005. This Act affected Section 9 of the Act No. 428/2002 Coll. (exemptions from restrictions as processing the special categories of personal data). The Office for Personal Data Protection rejected these changes in interdepartmental review and demanded that it would not be included in the Act on Personal Data Protection in such form, since the change was expected through a prepared Euro amendment in such manners proposed by the European Commission's expert.

The Slovak Ministry of Health, despite this clear requirement by the Office, prepared and without participation of the Office enforced indirect amendment to the Act No. 428/2002 Coll. on Personal Data Protection as amended by Act No. 602/2003 Coll.

Implementation of Directive 2002/58/EC

With regard to the fact the Directive 2002/58/EC set out the rights and obligations within the scope of the data protection specifically for the electronic communications area, it has been implemented into the Act No. 610/2003 Coll. on Electronic Communications within the scope of the New Regulatory Package for Electronic Communications. Responsibility for this Directive belongs to the Ministry of Transport, Posts and Telecommunications of Slovakia.

The Act on Electronic Communications was effective from 1 January 2004, thus Slovakia fulfilled an obligation to harmonise Slovak legislation in time. Personal data protection and protection of privacy is included in the 4th part of the Act.

Obligations of undertakings in protection of privacy and questions on unsolicited communication are included in the mentioned part as well. The Act inter alia gives the Telecommunications Office of Slovakia a role of National Regulatory Authority for electronic communications with a power to impose sanctions in case obligations resulted from the act are not fulfilled.

The European Commission has reviewed a full implementation of the New Regulatory Package Directives into the Slovak legislation. Within this context the Commission has noticed some shortcomings in the 10th Implementation report (European Electronic Communications Regulation and Markets 2004) on electronic communications legal acts issued in November 2004. At the beginning of the year 2005, the European Commission sent an official notice on incomplete transposition of the Directive 2002/58/EC. Notification has concerned missing provisions on 'cookies' and incomplete provisions on unsolicited communication. Slovakia has answered in a given time period and has proposed a solution. Currently an amendment of the Electronic Communications Act is being prepared and all missing provisions will be supplemented into this act. The amendment is in the legislative process and it is expected to be effective by 1 January 2006.

B. Major case law

Since the case law (precedential/decisional right) is not exercised in Slovakia, some cases are presented here that might be typical for candidate countries or new Member States of the European Union.

Illegitimate publication of personal data

The complainant was a candidate for judge of the Special Court. The subject of the complaint was a suspicion of unauthorised release of information about the fact that the National Security Authority did not close the security clearance/inspection of the data subject that was performed, in order to establish whether or not a nominee fulfilled the conditions stated in law for acquaintance with classified information, because of the alleged problems with proving the origin of the property. Information relating to the security inspection of the complainant was broadcast by a private television company in the main news. The data concerned, name, surname, employer and position can be considered as personal data for the purpose of this proceeding.

According to the Act No. 215/2004 Coll. on the protection of classified information and on the amendment and supplementing of certain acts, the National Security Authority is obliged to provide protection of registered data against unauthorised manipulation under Act No. 428/2002 Coll. on personal data protection.

This contribution as well as the above-mentioned facts prove that information related to the security clearance/inspection of the complainant were not officially announced (published) and approved by the National Security Authority.

It is more likely that the information was provided to television by a person, who learnt about it directly from the file of the National Security Authority or learnt about it from another person who had access to this information.

According to the Office, there is a justified suspicion that an unknown person made an unauthorised announcement or made the data, collected information about the complainant in connection with the execution of his security clearance by the National Security Authority, accessible by the unknown person, and thus the person accomplished elements of some of the crimes.

Under Section 38 paragraph 1 subparagraph j) of the Act No. 428/2002 Coll. followed by Section 38 paragraph 2 of this Act, the chairman of the Office submits a notification to the law enforcement agencies in the case of a suspicion that an offence was committed.

Based on mentioned facts, the Office notified the authorities in criminal proceeding of a suspicion that an offence was committed.

Unauthorised dealing with personal data of data subjects (aggrieved persons) - successional legal entity.

At the beginning of July 2003, a complaint was filed against a joint stock company in Bratislava at the Office for Personal Data Protection. The complaint was filed by a private research institute in Bratislava. The subject of the complaint was a suspicion that the joint stock company had violated the Act on personal data protection and was processing the personal data of data subjects without legal base. These activities were connected with the processing of personal data of affected persons and certificated experts; the information included title, name, surname, address, and results of theoretical and practical exams on protocols on exams.

It resulted from the motion that a private research institute, which filed a complaint, had become a legal successor of the state organisation, whose object of business was also providing a training and certification of experts.

The Office carrying out the inspection of the manners of receiving and processing the personal data found out that a joint stock company processed the personal data without a legal basis and was therefore in violation of Section 7 paragraph 1 and 3 of the Act on Personal Data Protection (in violation with Article 7 subparagraph a) and Article 7 subparagraph c) of Directive 95/46/EC). The joint stock company did not become the legal successor of the state-owned organisation and therefore was not entitled to use the rights to documentation on certificated personnel. This means it should not have processed the documentation as a controller appointed under special Act No. 264/1999 Coll. on technical requirements for products and conformity assessment and amendments as contained in later regulations. A joint stock company during the execution of controls did not prove that it has consent of data subjects, certificated personnel, since individual data subjects did not ask a joint company to issue a certificate and did not provide their own protocols individually or collectively.

Regarding the fact that violation by a specific person, i.e. a former employee of the state organisation, was detected during the investigations, the Office followed Section 38 paragraph 1 subparagraph j) of the Act on Personal Data Protection and informed the authorities active in criminal proceeding about committing the crime by a specific person under Section 257a and Section 178 of Criminal Code. Section 257a of the Criminal Code stipulates the punishment for the specific person, who will be proven to have deliberately misused the list on the information carrier, and Section 178 of the Criminal Code stipulates the punishment for the specific person who is proven to have communicated or allowed access to personal data gathered in connection with his profession, employment or office and thus breaches the confidentiality.

C. Major specific issues

Complaint about processing personal data by the Nation's Memory Institute of Slovakia

During the year 2004, the Office had been solving the complaint of data subject in the case of the processing of personal data by the Nation's

Memory Institute (Nation's Memory Institute is a public institution established by the Act on Nation's Memory. Under the Act, its aim is to make the documents on activities of security units of the state in 1939-1989 accessible).

The data subject claimed in its complaint that the Slovak Information System had delivered a personal file of the Nation's Memory Institute in an unauthorised way and without its knowledge and consent.

Under Section 7 paragraph 6 of the Act No. 428/2002 Coll., processed personal data of the data subject can be provided, made accessible or published from information systems with just a written consent. This shall not apply when it is necessary for criminal justice agencies to perform their tasks or when personal data are supplied to an information system on the basis of a separate law that lays down a list of personal data, the purpose of their processing and conditions of providing, making accessible or publishing personal data, and also legal entities, natural persons or entities abroad that have personal data provided or made accessible.

Such a separate Act is the Act No. 553/2002 Coll. on declassification of documents concerning activities of security bodies of the state in the period 1939-1989 and on establishment of the Nation's Memory Institute and amending and supplementing certain other acts (hereinafter: Act No. 553/2002 Coll.). According to Section 27 paragraph 1 of the Act No. 553/2002 Coll., the Ministry of Interior of Slovakia, the Ministry of Defence of Slovakia, the Ministry of Justice of Slovakia and the Slovak Intelligence Service shall hand over the documents on the activity of the security authorities in their ownership, possession or administration to the Institute, within eight months from the effective date hereof. From the above-mentioned, it results that Slovak Intelligence Service did not breach the Act No. 428/2002 Coll. by handing over the file of data subject, the Nation's Memory Institute.

The complainant also protested in his complaint that the Nation's Memory Institute owns, handles, and intentionally holds his personal file in an unauthorised way.

The complainant also states that under Section 20 paragraph 1 subparagraph e) of the Act No. 428/2002 Coll., he asked the Nation's Memory Institute for the return of his personal file.

The purpose of processing the personal data is stipulated in Section 1 subparagraph b) of the Act No. 553/2002 Coll. and it is recording, collecting, disclosing, publishing, managing and using documents of security authorities of the German Third Reich and of the Union of Soviet Socialist Republics, as well as security authorities of the State, which were created and collected in the period from 18 April 1939 to 31 December 1989 (hereinafter: crucial period) regarding crimes committed against persons of Slovak nationality or Slovak citizens of other nationalities.

From the above-mentioned results, the rights of a data subject under Section 20 paragraph 1 subparagraph e) of the Act No. 428/2002 Coll. shall be claimed after termination of the purpose of the personal data processing. In this case, the purpose of the personal data processing was not terminated and therefore the Nation's Memory Institute, as the controller, was not entitled to return the requested files and was obliged to keep processing this personal data under Act No. 553/2002 Coll.

Receiving the personal data essential for achieving the purpose of the processing by copying, scanning, or other recording of the official files on the carrier in the telecommunication sector

In 2003 and 2004, the Office received several complaints concerning the personal data processing by controllers acting in the telecommunication field.

The problem of processing the personal data in the sector of telecommunications was regulated by the Act No. 195/2000 Coll. on Telecommunication as amended (hereinafter: Act No. 195/2000 Coll.), which was replaced by Act No. 610/2003 Coll. on Electronic Communications (hereinafter: Act No. 610/2003 Coll.) and which came into effect on January 1, 2004. Both these acts were considered to be separate for the purpose of the Act No. 428/2002 Coll.

Act No. 195/2000 Coll. did not contain the necessities required by the Act No. 428/2002 Coll. Despite this fact, the controllers were entitled to process the personal data of data subjects to such an extent necessary in order to achieve a determined goal, since the provision of Section 52 paragraph 2 of the Act No. 428/2002 Coll. entitled them to do so.

The Act No. 610/2003 Coll. included the necessities required by the Act No 428/2002 Coll., namely the list of personal data, the purpose of their processing, conditions for their receiving and the circle of data subjects and amended the personal data processing in several provisions.

The Office dealt with the problem of requiring and copying official files and requiring other documents before providing telecommunication services.

An inspection proved that the controller violated the Act.

No. 428/2002 Coll. under Section 10 paragraph 6 of the Act No. 428/2002 Coll., which stipulates that "the personal data necessary for achieving the purpose of the processing may only be obtained by photocopying, scanning or other recording of official documents on an information carrier upon a written consent of the data subject or if a special Act expressly permits their obtaining without a consent of the data subject. Neither the controller nor the processor may force data subject's consent or make it conditional with a threat of rejecting the contractual relation, service, goods or duty of the controller or processor laid down by law."

During the inspection, it was found out that the authorised person of the controller breached this provision and also the working procedures issued by the controller when obtaining the personal data for the purpose of this agreement from the submitted documents, and then made copies of these official documents without asking for the consent of the data subject. At the same time, it was found out and proved that the controller had processed the copies of official documents without written consent of the data subjects.

In connection with processing the copies of official documents, it was discovered and proved that the controller had also obtained and processed personal data of other persons than participants and users, which were not necessary for achieving the above-mentioned purposes stipulated by the Act No. 610/2003 Coll., and thus breached the provision of Section 6 paragraph 1 and 3 of the Act No. 428/2002 Coll.

The inspection found out and proved that the controller processed the copies of official documents, which contained not only personal data of the data subjects signing the agreement with controllers, but also personal data of other data subjects without their consent. Making a

photocopy, for example of a wedding certificate, the controller obtained also personal data of other data subjects, including a birth number, which are not, in their extent and content, compatible with the purposes of the processing within Act No. 610/2003 Coll. and the manners of processing and using do not correspond with the purpose of their processing.

The photocopies taken from the execution of the inspection proved that controller had not ensured photocopying of personal documents to a necessary extent. When making the photocopies, he did not use any foils, which would cover those personal data, which were not necessary to achieve the purpose, for example the personal data of the wife, who is not a client of controller.

As there were not explicit consents of all data subjects on the photocopies whose personal data appeared on the photocopies, the controller had breached the provision of Section 7 paragraph 1 of the Act No. 428/2002 Coll., which stipulates that the processing of personal data may only be performed with consent of the data subject. The controller shall ensure demonstrability of the consent in such a way that a proof thereon can be presented.

The inspection did not find out any forcing or conditioning of the consent with the photocopies of official documents by an authorised person with a threat of rejecting the contractual relation, service, goods or duty of the controller or processor stipulated by law.

It was found out and proved that the controller asked for other documents with personal data of the data subjects. For example a military book, from which authorised persons were ordered by the controller to make photocopies.

Since the Office had suspicion of violation of a special Act, it asked the Defence Ministry of Slovakia to express its opinion on this problem.

The Defence Ministry approved the content of statement, in which the Office had proved the above-mentioned opinion that the personal identification card (former military card or military book – it is the same document) may not be enclosed as a supplement and handed over to an unauthorised person, since the personal identification card of the soldier is exclusively for the performance of his duties in order to show his membership to the armed forces and for needs of military register of citizens who perform their obligatory military service, and therefore may not be used for other purposes.

The data controllers were also warned of the fact that they had violated the provisions of the separate Act No. 162/1993 Coll. on Identity Cards as amended (hereinafter: Act No. 162/1993 Coll.), which stipulates that the identity card is a public document, which a citizen of Slovakia uses to show his identity, citizenship of Slovakia and other data recorded on the identification card, while he is not obliged to hand over another document to demonstrate the facts recorded in identity card, unless otherwise stipulated by this Act (Section 1 and 5 paragraph 2 of the Act No. 162/1993 Coll.).

The Office, based on the found and proved facts, issued the Provision, in which it imposed a duty on controller to harmonise processing of data with the Act No. 428/2002 Coll. and to re-elaborate the relevant methodical order, which also regulates the procedure of authorised persons of controller as requiring official and other documents and making copies.

Slovenia

I. GENERAL INTRODUCTION

A. Constitutional arrangement of protection of personal data in the Republic of Slovenia

The constitutional basis for adoption and contents of the Personal Data Protection Act of the Republic of Slovenia (of 2004) is Article 38 of the Constitution of the Republic of Slovenia dated 23 December 1991 (last amended on 23 June 2004), which stipulates:

"The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.

"The collection, processing, designated use, supervision and protection of the confidentiality of personal data shall be provided by statute.

"Everyone has the right to acquaint himself/herself with the collected personal data that relate to him and the right to judicial protection in the event of any abuse of such data."

Equally, the constitutional basis for the adoption of the Personal Data Protection Act in terms of the membership of the Republic of Slovenia in the European Union is laid down by the third paragraph of Article 3.a of the Constitution of the Republic of Slovenia, which stipulates:

"Legal acts and decisions adopted within the framework of international organisations to which Slovenia has transferred the exercise of part of its sovereign rights shall be applied in Slovenia in accordance with the legal regulation of these organisations."

From a general systemic viewpoint, the provisions of Article 38 of the Constitution of the Republic of Slovenia mean that those who drafted the Constitution chose the so-called 'processing model' in relation to the regulation of protection of personal data, and not the so-called 'misuse model', since that Article of the Constitution lays down general rules regulating appropriate (lawful) processing of personal data on the statutory level, and does not state the principled freedom of processing of personal data that can only be explicitly restricted by statute.

The second paragraph of Article 38 of the Constitution of the Republic of Slovenia lays down an obligation to regulate by statute the collection, processing, designated (purpose related) use, supervision and protection of the confidentiality of personal data. Specifically, this means not only the obligation to regulate the protection of personal data in a general (systemic) Personal Data Protection Act, but also the possibility of dealing with these issues in sectoral statutes (laws) that must also take account of the provisions of Article 38 of the Constitution of the Republic of Slovenia, and must therefore ensure an appropriate level of protection of personal data comparable to the provisions of the Personal Data Protection Act. Of course, the second paragraph of Article 38 of the Constitution of the Republic of Slovenia does not mean at all that all legal relations must be fully regulated in sectoral statutes in terms of protection of personal data. Firstly, because in the event of possible legal gaps in sectoral statutes, the provisions of the general (systemic) Personal Data Protection Act apply and prevail; secondly, because the Personal Data Protection Act or sectoral statutes define exceptions from the general regulation of protection of personal data, such as in cases of concluding contracts among private individuals.

The question of protection of personal data in the Republic of Slovenia was already posed as a constitutional/legal issue in the year of 1969 when the then Constitutional Court of the Socialist Republic of Slovenia sent a request for a review of constitutionality to the former Constitutional Court of Yugoslavia, concerning the decision of the then Federal Institute for Statistics of SFR Yugoslavia for obligatory collection of supposedly statistical data (school education and occupation of individuals, the body or organisation in which they were employed, the level of their income from individual sources, the number of members of their household and their incomes, and holiday homes and motor vehicles owned by individuals and members of their households) directly from individuals in connection with their incomes. The Constitutional Court of Yugoslavia decided in 1971[10] that "The Acting Director of the Federal Institute for Statistics was not entitled through his decision on collection of data on payers of contributions from joint revenues of residents for 1968 (Official Gazette of the SFRY, No. 55/68) to order the collection of data on payers of contributions from joint revenues of residents for 1968." and: "During the procedure and at the public hearing, it was found that on the basis of the acting director's decision, data were collected and processed relating to contributions from joint incomes of residents, thereby raising the question of the possibility and need to publish collected statistical data.

The Court did not get involved in this issue, because in its opinion to do so would exceed its powers. Whether the data mentioned shall be published or do accurately reflect the state of affairs, whether they are useful and other issues pertaining to publication should be a matter of special review and a special decision. But it clearly follows from the position of the Constitutional Court of Yugoslavia that these data were collected pursuant to acts that were not lawful.[11]"

After this Decision theoretical debates and scholarly contributions developed in the then Socialist Republic of Slovenia concerning the need to regulate personal data protection as a separate field of the right to privacy. For example, the terminology of personal data protection in the Slovene language was well established already in 1984 and is mostly still applied today in Slovene legislation and case law.

Following these debates, the Assembly of the Socialist Republic of Slovenia adopted on 27 September 1989 the Amendment XLIV[12] to the (1974) Constitution of the Socialist Republic of Slovenia, which was actually inserted as a new constitutional provision between Articles 209 and 210 of the Constitution, and which for the first time defined on a constitutional level the right to personal data protection:

1. "The protection of personal data shall be guaranteed. The collection, processing and designated use of personal data shall be defined by statute. The use of personal data in contravention of the purpose of collection shall be prohibited."

2. "This Amendment supplements Chapter IV of the second part of the Constitution of SR Slovenia."

[10] Decision of the Constitutional Court of Yugoslavia, Ref. No.: U 167/69, 17 March 1971.

[11] This Decision was adopted less than two years after the resolution of the Federal Constitutional Court of the Federal Republic of Germany in 1969 on the representative statistical census – the 'Mikrozensus' Case (27 BverfGE 1, 16 July 1969), which was sort of a starting constitutional law precedent that 'created' the legal foundations in the Federal Republic of Germany against unrestricted acquisition of personal data.

[12] Official Gazette of the SR Slovenia, No. 32/1989.

The seventh subclause of the first clause of Amendment LXVII to the Constitution of SR Slovenia, which was adopted on the same date as Amendment XLIV, stipulated that the Assembly of the SR Slovenia regulates the protection of personal and other data by statute.

Following Amendment XLIV to the Constitution, the first Personal Data Protection Act of the Republic of Slovenia was adopted in 1990, following several legislative projects in this respect that had been 'on the table' at least since 1983 in the then Socialist Republic of Slovenia. The Republic of Slovenia was therefore the only state of former Yugoslavia that regulated data privacy. This Act started to operate de facto at the end of 1991 (after police and defence legislation were partially harmonised with it) and more in 1992, when the first Personal Data Protection Inspector started to perform his supervisory functions.

On 24 October 1995, the European Union adopted 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, through which it regulated both protection of personal data and free movement of personal data within the European Union, which had to be done at the level of the European Union in order to enable the free movement of goods and services and to ensure at least approximately the same level of protection of personal data in all of the Member States of the European Union.

Some discussions within the Republic of Slovenia concerning the implementation of this Directive in the legal order of the Republic of Slovenia had started already in 1996, while the Draft of the Directive 95/46/EC as of 1990 was already unofficially translated in Slovene language in 1992.

In 1999, the National Assembly of the Republic of Slovenia (the Parliament) adopted the new Personal Data Protection Act that was mostly harmonised with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981[13] that was ratified by the Republic of Slovenia on 25 January 1994. In 2001, this Act was amended with an aim to harmonising it with provisions of Directive 95/46/EC. An important feature of this amended Act (status of 2001) was that it regulated two bodies concerned with the data protection supervision in the Republic of Slovenia – the Human Rights Ombudsman and the Personal Data Protection Inspectorate of the Republic of Slovenia – as a body within the organisation of the Ministry of Justice of the Republic of Slovenia. The Human Rights Ombudsman was proclaimed by this amended Act to be the independent supervisory institution for personal data protection but it had no direct (concrete) powers to perform this supervision. While, on the other hand, the Personal Data Protection Inspectorate of the Republic of Slovenia had direct powers of supervision concerning personal data protection, but it was not independent per se – its decisions and rulings (of first instance) could be appealed to the Minister of Justice (second instance) who could amend them, quash them or return to the Inspectorate. The right to judicial review was provided for aggrieved parties for lodging administrative disputes before the Administrative Court of the Republic of Slovenia (a specialised branch of jurisdiction / a specialised court for administrative law matters) and appeals could be filed before the Supreme Court of the Republic of Slovenia (the Administrative Law Department).

[13] CETS No.: 108.

B. Case law in the period of 1992-2003

Summarily, it can be stated that the principal actor in creation and establishing of case law concerning the protection of personal data in the Republic of Slovenia in the period of 1992-2002 was the Constitutional Court of the Republic of Slovenia. In 1992[14] it quashed a provision in the rules for issuing identity cards, due to the lack of statutory basis – obligation for producing fingerprints of an individual were not stated in the Act on Identity Card, but in the by-law – rules issued for this obligation. This provision was declared to be unconstitutional and unlawful.

In 2000, the Constitutional Court decided[15] that some provisions of the Act on the Radio Television of Slovenia were unconstitutional, because they allowed for disproportionate collection and use of personal data for purposes of obligatory payments of subscription to (public) Radio Television of Slovenia. It explicitly stated, "The right to privacy of the individual ends only then and there, where it collides with statutorily attested stronger interest of others."

In 2002, the Constitutional Court also decided[16] that the provisions of Act on the Central Register of Population concerning the processing of the standardised personal registration number (acronym EM_O in the Slovene language), which every citizen of the Republic of Slovenia receives obligatorily by the state, are not unconstitutional.

It stated that the standardised personal registration number does not pose such danger that it could not be required to be processed by the state. It was also stated that there is no special danger due to the fact that the filing system, in which this number is obligatorily included (the Central Register of Population), is managed by the Ministry of Interior, since there are other appropriate safeguards in the then Personal Data Protection Act of 1999/2001 (prohibition of the applying the same connecting codes for acquiring personal data from filing systems of public security, national security, defence, etc.). It was also stated that in cases when data privacy is involved, the proper standard for the constitutional review of legislation that regulates this sensitive area is strictness and precision. The test of proportionality was applied.

In 2002, the Constitutional Court also reviewed the constitutionality of the Census Act for 2001 and decided[17] that the question in the population census about the religious confession of an individual is not unconstitutional encroachment on the rights for separation of state and religious communities (Article 7 of the Constitution), freedom of conscience (Article 41 of the Constitution), the right to privacy (Article 35) and the right to protection of personal data (Article 38). Individuals who should provide such a statement had the right to refuse such a statement and statements on absent persons, younger than 14 years could only be provided by their written consent. However, it also decided that the data collected by the census for statistical purposes cannot be used for other administrative purposes.

[14] Decision of the Constitutional Court of the Republic of Slovenia, No. U-I-115/92, 24 December 1992.
[15] Decision of the Constitutional Court of the Republic of Slovenia, No. U-I-238/99, 9 November 2000.
[16] Decision of the Constitutional Court of the Republic of Slovenia, No. U-I-69/99, 23 May 2002.
[17] Decision of the Constitutional Court of the Republic of Slovenia, No. U-I-92/01, 5 March 2002.

Other decisions of the Constitutional Court are not mentioned here, for example concerning tax-related personal data, since they follow the described pattern of the Constitutional Court's decision-making and argumentation.

In 2002, the Supreme Court confirmed[18] the conviction of an official person for the abuse of personal data (Article 154 of the Criminal Code) and it also provided an interpretation of this criminal offence in relation to the Personal Data Protection Act.

In the year of 2003, the Constitutional Court adopted an important Decision concerning patient's access to his health data. It was decided[19] that in some specific circumstances this right can be denied when it is urgent for averting the harmful consequences for the patient's health status. The test of proportionality was applied.

There are some more decisions of courts of regular and specialised jurisdiction on personal data protection, but since they have not stated really important principles of data protection, they shall not be presented in this Report.

II. MAIN DEVELOPMENTS IN THE REPUBLIC OF SLOVENIA IN THE YEAR OF 2004

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

Around May 2003, detailed discussions started with the appropriate body of the European Commission (with the then Media and Data Protection Unit DG Internal Market) concerning the proper harmonisation of Slovenia's Personal Data Protection Act with provisions of Directive 95/46/EC. Drafting of amendments to the existing Act of 1999 started in July 2003 at the Ministry of Justice of the Republic of Slovenia and in November 2003 a decision was reached that an entirely new Personal Data Protection Act is needed for proper harmonisation with the Directive 95/46/EC. The provisions of the Draft Act were drafted by the experts of the Ministry of Justice and the Inspectorate for Personal Data Protection of the Republic of Slovenia. Then the Draft Act was submitted to inter-departmental (inter-ministerial) consultations and to the opinion of the Legislation Service of the Government at the beginning of March 2004, continuously discussed in details with the appropriate body of the European Commission, and also the Human Rights Ombudsman and the Commissioner for Access to Information of Public Character submitted opinions. On 25 March 2004, the Government of the Republic of Slovenia submitted the Draft Personal Data Protection Act to the National Assembly of the Republic of Slovenia, where the Draft Act went through three readings and was adopted on 15 July 2004[20]. It entered into force on 1 January 2005.

In the meantime, the Republic of Slovenia became a Member State of the European Union on 1 May 2004.

[18] Judgment of the Supreme Court of the Republic of Slovenia, Ref. No.: I Ips 121/2000, 11 December 2002.
[19] Decision of the Constitutional Court of the Republic of Slovenia, No. U-I 60/03, 4 December 2003.
[20] Official Gazette of the RS, No. 86/2004.

The main purpose of the new Personal Data Protection Act of the Republic of Slovenia was harmonisation with provisions of Directive 95/46/EC, which was achieved by the adoption of this Act.

The new Act abolishes any appeal jurisdiction or influence of the Ministry of Justice on the supervision in field of personal data protection, the current Inspectorate for Personal Data Protection of the Republic of Slovenia transitionally remains within the organisation of the Ministry of Justice, but performs already most of the jurisdictions and powers of the independent data protection supervisory authority (with the exception, for example, of direct access to the Constitutional Court). The new State Supervisory Body for Personal Data Protection, into which the Inspectorate should be transformed, should start to operate fully as an independent body (outside the Ministry of Justice) on 1 January 2006. The independent Human Rights Ombudsman retained some advisory functions and supervisory function over the work of the State Supervisory Body for Personal Data Protection.

The Act distinguishes a bit between the processing of personal data in the public sector and in the private sector.

Other important features of this Act is sectoral (specific area) regulation of video surveillance, biometrics, direct marketing, public books (registers), lists of visitors, expert supervision and linking (interconnecting) of filing systems.

Decision-making on transfers of personal data to third countries and decision-making on whether third countries ensure an adequate level of protection of personal data is within the jurisdiction of the Inspectorate.

Also, it is within the jurisdiction of the Inspectorate to manage the register of filing systems, but currently the Ministry of Justice still provides technical aid for its managing.

Concerning the Directive 2002/58/EC it can be stated that it was implemented by the Electronic Communications Act[21] that was adopted on 9 April 2004 and entered into force on 1 May 2004. Chapter X of this Act mostly regulates the protection of personal data, privacy and confidentiality in electronic communications. The transitional provision of the new Personal Data Protection Act abolished the standardised personal registration number (acronym EMŠO in Slovene language) from the provisions of the Electronic Communications Act on phone directories, since due to the mistake of the legislator it was obligatory to publish it in phone directories. Also, since the tax number was already stated in the provision of this Act to be collected and processed for the use of payments of phone bills, it was assessed that the processing of the standardised personal registration number by providers of electronic communications services for payments of phone bills would then be disproportionate and subsequently the standardised personal registration number was abolished from the Electronic Communications Act also due to that reason.

[21] Official Gazette of the RS, Nos. 43/2004 and 86/2004.

B. Major case law

Important decisions of the Inspectorate for Personal Data Protection of the Republic of Slovenia in 2004 concerned several areas.

For example, in the case of the Bank of Slovenia (the central bank), the Inspectorate prohibited the publication of the register of banking accounts on the Internet, until the so-called data tracking (to whom the transfers of data are made, which data were transferred, on what legal basis and when) shall be guaranteed. Data concerned were obligatorily transferred from business banks which sent data on their clients – the information on natural persons such as name, surname, address, tax registration number, the number of the account, etc.; this register was therefore composed/established from bank accounts that were opened in business banks. The purpose of this register available via the Internet to anyone, regardless of any showing of legal interest or use of password, was supposedly easier enforcement of civil judgments and easier acquiring of data for actions of private parties before courts. However, this purpose was not explicitly stated in the Act in question. The Ministry of Justice, who was then still competent for solving appeals, changed the decision of the Inspectorate and prohibited any processing of personal data of natural persons in this register on the Internet, due to the non-existence of the statutory purpose of processing them. Articles 2 (b), 6, paragraph 1 (b) and 5 (b) of the Directive 95/46/EC were used as an argument in this second Decision. The constitutionality of the publication of this register on the Internet is currently also being decided by the Constitutional Court.

Another important case for the Inspectorate in 2004 was the case of tax administration. The Inspectorate prohibited the use of improper envelopes for sending decisions on tax liability to tax subjects (natural persons), since they were so transparent, that the contents from envelopes could be read by using normal light. It was also decided that the data controller (the tax administration) was not relinquished of its liability for legal processing of personal data, just because it had concluded a contract on contractual processing with the processor. The Inspectorate also issued a proposal for minor offence proceedings against the responsible person within the tax administration to the minor offence judge. An appeal by the tax administration to the Ministry of Justice was unsuccessful; in its Decision the Ministry also quoted the Directive 95/46/EC on the processor.

Even some lectures or non-binding opinions by the Acting Chief Personal Data Protection Inspector had some effect in public. His lecture from December 2003 to the police resulted in the end of practice for the police publicising personal data on natural persons in cases of criminal denunciations. There were some strong disapproving reactions by the media. However, the Inspector stated that it was possible to publicise such personal data in case, if the expert public opines, such publication is needed and that in such case it should be precisely regulated in legislation, with taking in due account specific circumstances like the right to the presumption of innocence.

A similar effect was achieved by his public statement in 2004 concerning the practice of some courts publishing on the Internet the personal data of parties partaking in court proceedings. The practice was mostly stopped and the Courts Act was therefore changed accordingly in 2004, allowing for limited publication of such personal data. As a result, only a name and a surname of a party to a

judicial proceeding (only for those proceedings that are not closed from the public) can be now published on a court board and they may also be published in electronic form in such manner as will make them accessible to the public (not necessarily on the Internet). It is also provided that the name and surname of a judge or a Chairman of the court panel shall be published in the same manner – in relation to the specific court case upon which she/he is adjudicating. Besides that, the reference number of the case shall be published and general description of the matter, date and time of the beginning of the hearing or session, and locality and place about which the parties to judicial proceedings should be informed.

C. Major specific issues

The biggest issue where slow progress in the area of protection of personal data is shown is the health sector – the security of personal health data (which are sensitive data according to the Personal Data Protection Act). However, co-operation of the Inspectorate with appropriate health institutions in the area of information technology might accelerate this progress. On the other hand, it can be stated as a positive aspect that the processing of personal data in the health sector is regulated in great detail by the health legislation.

Currently, another important issue is the insufficient number of Inspectors for Personal Data Protection, but this should be remedied in the near future.

Important projected activities for the future are preparations of sectoral guidelines for certain kinds of processing of personal data, like video surveillance and recommendations for processing of health data in the health sector.

There are also significant preparations in the Republic of Slovenia concerning the personal data protection and the Schengen acquis.

New developments, especially in the year of 2004, were some conflicts on the practical and theoretical level between the right to personal data protection (Article 38 of the Constitution) and the right to access to information of public character/freedom of information (Article 39, paragraph 2 of the Constitution), concerning the Act on Access to Information of Public Character, adopted in March 2003 and substantially amended in July 2005. The Personal Data Protection Act provides for a special procedure for resolving those conflicts in proceedings before the Administrative Court of the Republic of Slovenia.

On the governmental level, it is currently considering whether to unite areas of personal data protection and access to information of public character in one body – the Information Commissioner. Therefore the current Inspectorate for Personal Data Protection of the Republic of Slovenia (the future State Supervisory Body for Personal Data Protection) and the current Commissioner for Access to Information of Public Character would be united in one institution. That institution would nevertheless be completely independent from the executive and legislative authority; its head would be appointed by the National Assembly of the Republic of Slovenia, upon the proposal of the President of the Republic.

Spain

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

The European Parliament and Council Directive 95/46/EC was incorporated into Spanish legislation under Organic Law 15/1999 on the protection of personal data (LOPD).

In terms of the norms that develop the Personal Data Protection Act and in order to provide greater transparency to the activities carried out by the Spanish Data Protection Agency, the Instruction (secondary legislation) 1/2004 was approved regarding the publication of resolutions, and passed as a consequence of the modification introduced by Act 62/2003 on Fiscal, Administrative and Social Order Measures, which establishes the publication of the Spanish Data Protection Agency (Agencia Española de Protección de Datos – AEPD) resolutions once the interested parties have been notified.

On the other hand, some of the priorities of the AEPD for 2004 were the start of works aimed at the drafting of a General Regulations implementing LOPD. In addition, new Agency Statutes have started to be drafted in order to replace the approved Royal Decree 428/1993 as a result of the application of the LOPD and new competences assigned by the General Telecoms Act and the Information Society Services and Electronic Commerce Act; hence an expansion of the AEPD headcount has been approved to 15.59% as a result of the assumption of these new responsibilities.

In addition to the regulatory development of the Organic Data Protection Act, the legal framework that it provides is complemented by several general or sector regulations of diverse regulatory scopes, which represent the applicable legal framework on this matter. Among such regulations, it is worth highlighting the following:

- Royal Legislative Decree 2/2004, 5 March, which approves supplementary legislation of the Local Treasury Office Regulatory Act
- Royal Legislative Decree 6/2004, 29 October, which approves supplementary legislation of the Private Insurance Order and Supervision Act
- Royal Decree 183/2004, 30 January, which regulates the individual healthcare card
- Royal Decree 2393/2004, 30 December, which approves the Regulations of Organic Act 4/2000, 11 January, regarding the rights and freedom of foreigners in Spain and their social integration
- Royal Decree 424/2005, 15 April, which approves the Regulation implementing the General Law of Telecommunications GLT (Transposition of the Directive 2002/58/CE). This important regulation sets out principles of data protection in different spheres of telecommunications:

  ➔ traffic data, invoicing and location of the subscribers and users processing by telecom-operators

  ➔ unsolicited commercial communications

  ➔ elaboration of the subscribers' telephone number directories and the benefit of advanced services of telephony, like the identification of the line of origin, and the automatic deflection of calls

- Regional regulations
Act 2/2004, 25 February, regarding Public Owned Personal Data Files and the Creation of the Basque Data Protection Agency.

European Parliament and Council Directive 2002/58/CE of 12 July 2002 governing the processing of personal data and the protection of privacy in the electronic communications sector, which has expressly overridden and replaced Directive 97/66/CE, had been incorporated into Spanish legislation through General Telecommunications Law 32/2003 of 3 November.

B. Major case law

As provided in section 48.2 of the Spanish Data Protection Law, the Director's decisions end the governmental process. Therefore, and regardless of the presentation of a reposition appeal, such resolutions can only be challenged administratively. In 2004, a total of 84 rulings were passed by the High Justice Tribunals and National High Court and nine rulings by the Supreme Court resolving appeals to unify the doctrine. In this text, reference is only made to the paragraphs that establish precedents for controversial matters and data protection aspects that are difficult to interpret:

Use of traffic and invoicing data without consent and applicability of the LOPD to professionals

The Ruling dated 11 February 2004 resolved the appeal confirming the criteria held by the Agengy whereby a telecoms operator was sanctioned for the use of professional traffic data for incompatible purposes without the consent of the data owner and its assignment to third parties. The commercial promotion of these services and products is authorised to process traffic and invoicing data for the commercial promotion of its own telecom services as long as the subscriber has previously given his consent.

Breach of the obligation to provide the right to cancel

Ruling passed on 3 April 2004 confirms the doctrine of the Spanish Agency, rejecting the appeal presented against the Agency's resolution due to a breach of LOPD section 16, regarding the cancellation of data, given the cancellation requested by the interested party had not been executed. The acting party considered that the 'cancellation' referred in LOPD section 16 did not represent the destruction or physical deletion but that data should be blocked through a password; however the courtroom reviewed the arguments and understands that the date on which the data was blocked has not been accredited or confirmed.

Sending of SMS without consent and express prohibition of the interested party

Ruling passed on 17 March 2004 confirmed the Agency's resolution regarding the breach of right to consent. The appellant processed personal data with the remission of a publicity message to a mobile phone with the express prohibition of the affected, which had been provided two months before the campaign, sufficient with the existing technical means to cancel the data. The Courtroom considered it was reckless to initiate a publicity campaign in the knowledge of a future breach of customer rights.

Applicability of LOPD to files and non automated processing

The Ruling passed on 19 May 2004 rejects the appeal presented against the Agency's resolution due to breach of the duty to secrecy.

The Spanish Data Protection Law is applicable to both automated and non automated files, adding that under no circumstances can the acting party resort to this adaptation period, as the First Additional Provision of the Data Protection Law refers to files created before the effective date of said Act.

Obligation to accredit the consent of interested parties for the processing and cession of their data

A Ruling was passed 30 June 2004, which rejected the appeal presented against the Agency's resolution for the breach of Sections 11 and 6.1 of the LOPD (regarding the cession and consent), is founded on the doctrine already evidenced in rulings of 24 January and 9 May 2003 with regards to the need of accrediting the reception by the affected party of notices sent by the person responsible for the file.

Data processing by third parties and outsourcing

The Ruling passed by the Administrative Court of the National High Court on 21 July 2004 partially accepts the appeal presented against the Agency's resolution dated 26 September 2001. The Court analysed Article 12 of the LOPD examining the joint and several responsibilities of the company stated in the LOPD that must establish the obligations to be complied by several parties, and if appropriate, regulate in which cases a certain person or entity is responsible for preventing the administrative breach, supposedly committed by one or more persons and not determine it generically without sufficient detail in terms of definition in scope and meaning required by a charge of this nature.

Application of Royal Decree 994/1999, 11 June, to files and processing carried out by doctors

The Ruling passed by the Administrative Court of the National High Court on 20 October 2004 rejects the request dated 20 May 2002, resolving that computer files and processing performed by doctors regarding the health of their patients are subject to Organic Act 15/1999, 13 December and the Regulations of Security Measures.

Insertion of data in a credit worthiness file

The Ruling passed by the Administrative Court of the National High Court on 1 December 2004 accepts the appeal presented against the Agency's resolution for breach of section 4.3 of the LOPD.

It is a case of insertion of customer data in a credit worthiness file. The challenged resolution considers that the appellant has breached the principle of data quality, as it added the details of the claimant in a credit worthiness file with regards to a debt that was not true, due and demandable, as there were doubts regarding the existence of such debt. The Agency considers this is a case of associated contracts, under the protection of Act 7/1995, Retail Loans, and therefore, as the contract is ineffective, the existing debt is not effective.

C. Major specific issues

Transparency

Before Parliament – Hearing at the Constitutional Commission of the Chamber of Deputies

In December 2004, the Director of the AEPD was heard, by own initiative, by the Chamber of Deputies for presenting the annual report of this AEPD and answering related questions of the deputies, such as:

- Normalisation of the personal data protection culture
- Regulatory development of Act 15/1999, 13 December, of personal Data (LOPD)
- The staff and means increase for the Agency
- The boosting of preventive actions: Ex officio sector plans and Standard Codes
- The promotion and improvement in co-operation between AEPD and regional data protection agencies
- The intensification of the Agency's international presence.

Before citizens – Publication of all AEPD resolutions

As has already been mentioned regarding the implementation of Directive 95/46/EC, in order to provide greater transparency to the activities carried out by the AEPD, an Instruction (secondary legislation) 1/2004 was approved regarding the ordering of the publication of the final resolutions of the Agency.

Enforcement

- *Fight against Spam*

It is important to highlight the relations of the AEPD with the United States, through the Federal Trade Commission, concerning undesired commercial communications (or 'Spam') in order to establish instruments that contribute to greater effectiveness in the fight against Spam, whose competence in Spain falls on the AEPD after the General Telecoms Act gave it these responsibilities. During 2004, contacts were established with said Federal Commission in order to establish a specific line of co-operation that was specified in the negotiation of a 'Memorandum of Understanding'. (At the moment of closing this annual report, it is already signed.)

- *The boosting of preventive actions: Sector inspections during 2004*

In order to promote preventive actions, one of the fundamental activities of the Data Protection Agency is Sectorial Inspection Programmes, which annually audit various sectors of both public and private standing, giving rise to the issue of the corresponding Recomendations that must be fulfilled in a mandatory fashion, so as to bring into line the treatment given by said sectors to the requirements laid down in the data protection legislation.

In 2004, the conclusions and recommendations regarding Sectorial Inspections carried out at the National Public Office Institute (INAP) and Hospital Laboratories were approved.

➔ INAP (Instituto Nacional de Administración Pública – National Institute for Public Administration)

The organisation is in charge of promoting and developing policies for training, perfecting and research within the scope of the Central Government. During 2003, INAP carried out over 1 000 actions involving more than 23 000 students and 3 000 teachers, figures that show the volume of personal data processing performed.

In general, the information and documentation obtained by INAP is suitable and pertinent, however it was recommended to establish a documented procedure that facilitates the right of access, rectification and cancellation.

➔ Hospital Laboratories

During the sector inspection carried out in 1996 to public hospitals, it was detected that external entities participated in their laboratories that could access personal data. During the years 2003 and 2004, a new sectorial inspection was carried out to analyse in depth how said accesses were performed; the conclusions and recommendations of the inspection were approved in 2004. This inspection presents, therefore, a very specific characteristic, as it focused on the aspects regarding security measures in the conditions of access by third parties. The inspection is complemented with a recommendation regarding the exercising of the rights to access, cancel and oppose regarding data protection regulations and healthcare regulations.

- *Promotion of self-regulation*

During 2004, the Agency registered the following codes of conduct which self-regulate data protection in both public and private sectors.

➔ Code of conduct of Dental Surgeons and Stomatologists in Spain

This code of conduct, drafted by the Spanish General Council of Official Schools of Dental Surgeons and Stomatologists, defines specific rules for the processing of personal data within this professional scope; it establishes the conditions for the organisation, operating regime, applicable procedures as well as the rules for exercising the rights of said patients.

➔ Code of conduct of Castilla-La Mancha University

The purpose of this code of conduct is three fold: to comply with corresponding legislation in the easiest and safest way through a single document that includes all the essential elements, increase the protection of personal data stored in automated files increasing the legally required security measures, and serve as educational material for the university community, with special interest to students.

➔ Code of conduct of Catalan Association of Assistance Resources (ACRA)

The code of conduct is a quality distinction in the processing of personal data required to provide assistance services, for those associated that adhere to it, and a guarantee for residents and public offices, regarding the proper operation of the centre or establishment in terms of data protection.

➔ Type code for the Real Estate Mediation Sector (AEGI)

The essential objectives of this code are to help any customer know his rights, resolve any doubts that may arise in the implementation of the regulation of personal data protection, confer reliability and guarantees practical and operational standards used by companies associated to the processing of personal data and the implementation of the law.

Raising data protection awareness and promoting co-operation with regional agencies

Continuing with the activity of raising data protection awareness initiated in 2003, the Director of the AEPD has developed intense activity through his direct involvement in numerous meetings and sessions. In addition, in order to normalise the data protection culture, during 2004 the AEPD signed several co-operation protocols, both with public and private entities. The ONCE Foundation and

the Spanish Committee of Representatives of Handicapped People, the Association Comisión de Libertades e Informática and the Antonio de Nebrija University.

On another side, in 2004, the third regional Data Protection Agency was created; the Basque Data Protection Agency (with similar competeces to Madrilenean and Catalonian DPAs). To continue and promote the ruling institutional collaboration, a Co-operation Protocol was adopted between the AEPD and the three regional agencies for creating a communication system of exchange information of data processing notifications.

Spanish activities in the Ibero-American Data Protection Network

In the context of Ibero-America, efforts are also being directed at achieving co-operation and promoting personal data protection. As was noted in the last annual reports (2002-2003) the Ibero-American Data Protection Network was created by the initiative of the AEPD to achieve this goal.[22] The Spanish Data Protection Agency promotes the Ibero-America Data Protection Conference on an annual basis. In 2004, this conference was held in Cartagena de Indias (Colombia) in May.

The meeting in 2004 enjoyed the presence of more than 40 authorities and prominent representatives of public and private circles in 15 Ibero-American countries. During the work sessions, data protection in the financial sector was analysed, including the European and Ibero-American viewpoints regarding international data transfers, attacks to the privacy in the telecoms and Internet sector, fight against Spam and the use of financial information with marketing purposes in the commercial sector. The result of these meetings was the approval of several conclusions included in the final Cartagena Declaration that defines common positions regarding the matters covered in the meeting.

[22] More information about IDPN is available at: https://www.agpd.es/index.php?idSeccion=349. Also available in English.

Sweden

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

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

In February 2004, an inquiry, tasked with reviewing the Personal Data Act in order to see if a 'misuse model' could be applied to the PDA within the requirements of the EC Directive, presented its report. The inquiry proposed to exempt processing of personal data in unstructured material, such as continuous text, sound and images, etc. from the great majority of handling regulations in the PDA. The handling rules would thus not be applicable to everyday processing like the production of continuous text in word processing software, publication of such text on the Internet and e-mail correspondence, for example. The exemption would, however, only apply on condition that the information was not intended to be included in a database with a personal data-related structure. One simple rule would apply instead; processing would not be permitted if it would involve an improper intrusion on privacy. The proposal was submitted to consultation with different organisations and in an opinion of September 2004, the Data Inspection Board said that it approved the proposal in terms of exempting such processing that does not involve privacy risks from some of the rules in the PDA. The Board, however, criticised the proposed rules for being too complicated and feared that it would be difficult to decide whether the PDA should apply or not. The proposal is now under further consideration within the Ministry of Justice.

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

B. Major case law

Following the EC Court of Justice's preliminary ruling in November 2003, regarding disclosure of personal data on the Internet, the Swedish Göta hovrätt (a Court of Appeal) delivered its final ruling in the case in April 2004. The case concerned a person who, while volunteering as a youth leader in the Church of Sweden, had published personal data about other

employees and officials in the local organisation on the Internet without first obtaining their consent. Some of the data included health data. The purpose of the disclosure was to provide information to the children in an easy and humorous way. When finding out that some of the people that the information referred to disapproved, the information was deleted immediately. A district court found that the church volunteer had violated certain provisions of the Personal Data Act. The case was brought to the *Göta hovrätt* who decided to turn to the EC Court of Justice with questions regarding the interpretation of the EC Directive 95/46/EC. The Court of Justice found inter alia that the processing fell within the scope of the Directive and that sensitive data had been processed. However, according to the Court, the church volunteer's actions did not constitute a transfer of data to third countries. Further to this statement from the EC Court of Justice, the prosecutor later withdrew the charges in respect of transfer to third countries. In its ruling of April 2004, *Göta hovrätt* found that the church volunteer had contravened certain other provisions of the Personal Data Act by negligence. The Court found, however, that her offence constituted such a petty case that no sentence should be imposed.

In June 2004, the committee of the Data Inspection Board decided that collection and processing of students' fingerprints for the purpose of checking access to the school canteen was not adequate or relevant, and this regardless of the fact that consent would be obtained. Three of the committee's members, including the Director-General, expressed a different opinion and said that the processing was permitted on condition that valid informed consent was obtained from the students. The majority of the committee, however, took the view that the checks could be made in a less privacy-intrusive manner. This view has since been upheld in other similar cases of the Board. The Board's decisions have been appealed against in the county Administrative Court.

C. Major specific issues

In April 2004, Mr Göran Gräslund took office as the new Director General of the Data Inspection Board.

The Board has continued to carry out certain supervisory activities in the form of specific projects. Inspections have thus been made at several different controllers within the same sector and the results have been summarised in reports that have been published. In 2004 the Data Inspection Board published three reports that dealt with the following issues: banks and their handling of requests for right of access (2004:3), biobanks and the Personal Data Act (2004:2), and the processing of personal data within the local municipal administration of social services and environmental issues (2004:1).

The debate in Sweden during 2004 has highlighted the issue of personal data processing in relation to new technology, for example biometric data and RFID. A commission of enquiry proposed to widen the scope of using DNA-profiles in law enforcement and it was argued by some that Sweden should introduce a DNA-register covering the whole population for identification purposes regarding criminals as well as casualties in accidents. Another issue of debate was the increased video surveillance and proposals were put forward that the Data Inspection Board should have certain supervisory tasks in this field which currently falls under the supervision of the county administrative boards. Attention was also given to camera cell phones and the adherent risk that privacy-intrusive pictures are taken and made available on the Internet. The media also focused on the proposal at EU-level on regarding storage of traffic data. Finally, the issue of how to use information technology in health and medical care was discussed and the Board could see a tendency towards automated processing of sensitive data (electronic patients records, etc.) in larger systems and with wider access rules.

In terms of self-regulation, the Data Inspection Board gave opinions on two proposals for codes of conducts. One referred to an amendment of the existing code in market research activity and the other referred to debt recovery activity.

In April 2004, the Ministry of Justice set up an inquiry with the task to analyse existing legislation related to privacy and see if this legislation adequately protects privacy. The inquiry shall, in particular, analyse the relation between coercive measures and surveillance methods on one hand and the protection of privacy on the other. It shall also examine whether the constitutional provision on the right to privacy in relation to automated personal data processing needs to be amended so as to have the same legal implication as the provisions on other constitutional rights and freedoms. The inquiry consists of members of Parliament and privacy experts and they will present their results by the end of March 2007.

The United Kingdom

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

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

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

B. Major case law

During 2004 there has been no major case law in the UK courts relevant to Directive 95/46/EC and Directive 2002/58/EC.

C. Major specific issues

Following consultation on entitlement cards in the preceding year, the UK Government published its Identity Cards Bill in 2004. The Bill proposed a card with a biometrically enabled chip which would be underpinned by a central database containing a range of information about individuals. Information on the register would include name, date of birth, address, previous addresses, biometric identifiers and an audit trail of instances where identity is checked against the register.

The Information Commissioner has sought to inform and influence the discussion on the proposed identity card to ensure that it is compliant with the Data Protection Act 1998. To that end the Information Commissioner has responded to the Home Office consultation on the draft Identity Cards Bill, had discussions with the Home Office, gave evidence to the Parliamentary select committee inquiry into the proposals and also published a statement to inform the Parliamentary debate. The Information Commissioner has been keen to stress the problems, as he perceives them, with the scheme including the extent and relevance of the information that will be held, access to the database and the need for greater consideration of data protection safeguards.

The Information Commissioner has been in discussion with the Department for Trade and Industry to try to increase the powers available to him to help combat the unsolicited marketing e-mails that originate in the UK. The Information Commissioner recognises that this is an area that requires effective co-operation, and he has signed memorandum of understanding with other relevant bodies in the UK and also in Australia and the USA.

The Information Commissioner recognises the importance of preventing and dealing with child abuse cases and the need for professionals to share information in appropriate cases. However, there is a real concern about the proposal to set up databases – or indexes – of all children in the UK as outlined in the Children Act 2004. The Commissioner's concerns include; the rationale for such a far reaching scheme remains ill defined; there may be substantial difficulties in keeping the database secure and up-to-date; there is considerable uncertainty and potential for detriment with the use of 'cause for concern' indicators; and there is a real risk that the privacy of children and parents will be compromised.

During 2004, the Information Commissioner provided evidence to the following Parliamentary select committees:

- Home Affairs Select Committee inquiry into identity cards
- Constitutional Affairs Select Committee inquiry into the work of the Information Commissioner. This included the Information Commissioner's previous enforcement action against credit reference agencies and transferring personal data to processors based outside Europe.

During 2004, the Information Commissioner provided responses to the following government consultations:

- A review of the civil proceedings by and against the Crown, April 2004
- Statutory appeals and statutory review, April 2004
- Identity cards draft Bill consultation July 2004
- Policing: modernising police powers to meet community needs, October 2004.

Chapter Three

European Union and Community Activities

3.1. EUROPEAN COMMISSION

3.1.1. Eurobarometer

Two opinion surveys conducted by Eurobarometer during autumn 2003 were published early in 2004. One looked at EU citizens' views on privacy relating to information held about them by a variety of public and private organisations, and related data protection issues via face-to-face interviews. The other collected European Union companies' views about privacy via telephone interviews. The results showed a large awareness problem, both for citizens and business.[23]

3.1.2. Report on Switzerland

As requested by Article 4(1) of the Adequacy Decision 2000/518/EC, the Commission services have proceeded with an analysis of the application of this Decision by the Swiss authorities covering the period mid July 2000-mid April 2004. (Staff Working Document of 20 October 2004, SEC (2004) 1322[24])

The Commission services have not identified any major problems in respect of the current Swiss data protection system and take the view that the Swiss data protection system continues to provide an adequate level of protection of personal data within the meaning of Article 25 of the Directive. In particular, the Commission services are satisfied with the situation regarding international data transfers to third countries, since in case of transfer of data from Switzerland to countries that have not ratified the Council of Europe Convention 108, Article 6(1) of the Swiss data protection law requires the latter to provide protection equivalent to the one provided under Swiss law.

3.1.3. Report on Safe Harbour (United States of America)

On 20 October 2004, the Commission issued a report assessing the implementation of the Safe Harbour Decision ('Commission Staff Working Document, SEC (2004) 1323 - The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce'[25]). The report concludes that while the implementation of the Safe Harbour Decision in essence ensures the protection of individuals' privacy rights, shortcomings exist where improvement is needed for the decision to produce its full effects. Briefly, the following is a summary of the shortcomings identified in the report: (a) The report suggests that the Department of Commerce (DoC) should be more careful in scrutinising US organisations that self-certify to the Principles in order to avoid being listed in the Safe Harbour List of companies lacking a publicly available privacy policy. The Commission also considers this to be one of the instances where it is essential for the Federal Trade Commission (FTC) to be more proactive in monitoring organisations' compliance with the Principles and launching investigations where questions exist regarding Safe Harbour compliance. (b) Regarding the functioning of the DoC as the body competent for ensuring self-certification, the Commission feels that the DoC should implement various changes to its website which would, inter alia, enhance its transparency. (c) Regarding alternative recourse mechanisms, the report highlights certain shortcomings in the way they operate and, given their key role in enforcing the Safe Harbour scheme, suggests the need for such problems to be resolved rapidly.

[23] For the executive summary and the full report see http://europa.eu.int/comm/justice_home/fsj/privacy/lawreport/index en.htm#actions

[24] http://europa.eu.int/comm/justice_home/fsj/privacy/docs/adequacy sec-2004-1322_en.pdf

[25] http://europa.eu.int/comm/justice_home/fsj/privacy/docs/adequacy sec-2004-1323_en.pdf

3.1.4. Adequacy Decision on PNR data to the United States of America

Transfers of personal data to third countries must respect the requirements of Article 25, or, in the alternative, fall within the scope of the derogations from Article 25 permitted by Article 26. When considering the derogations under Article 26, the Working Party concluded that none of these provisions provided an appropriate basis for the transfer of air passengers' PNR data for the purposes of the US authorities.[26]

The Commission supported this view and adopted on 14 May 2004[27] a decision under Article 25 of Directive 95/46/EC stating that the United States' Bureau of Customs and Border Protection (CBP) ensures an adequate level of protection for personal data contained in the Passenger Name Record (PNR) of air passengers transferred from the European Union concerning flights to or from the United States. The decision is based on detailed conditions for processing PNR data set out in the Undertakings of CBP. The decision was taken after lengthy and difficult negotiations with the US.

The processing by airlines of PNR data in the EU – that is, its collection within the EU and its onward transfer to the US – is subject to the provisions of the Directive regardless of the nationality of the airlines concerned. This means that not only EU airlines are concerned with the PNR decisions, but all airlines which process personal data in the EU in view of flights from the EU to and from the US.

[26] Opinion 6/2002 at paragraph 2.5.

[27] OJ L235 of 6.7.2004, page 11.

3.2. COUNCIL

Transfer of air passengers' personal data to the US Bureau of Customs and Border Protection

In addition to the Commission adequacy decision, an international agreement was deemed necessary to authorise airlines to treat the US request for sending PNR data as a legal obligation under the Directive (Article 7 c). The Commission adequacy decision is limited to stating that an adequate level of protection is ensured and thus it could not address this issue. The Council adopted an international agreement on 17 May 2004[28] authorising airlines to transfer PNR data to US Customs, thereby providing airlines with the necessary legal basis for the processing of PNR data in the EU as a result of the US requirements.

3.3. EUROPEAN PARLIAMENT

Report on the First Report on the implementation of the Data Protection Directive

In March 2004, the European Parliament adopted a Resolution on the First Report on the implementation of the Data Protection Directive approved by the Commission in May 2003. The resolution was very supportive of the Commission's findings and called on all the actors concerned to co-operate and ensure correct implementation of the Directive. It also addressed other issues like the transfer of passenger PNR data to US authorities, the need for a comprehensive and trans-pillar European data protection regime, the concerns raised by exceptions to privacy laws and various other issues.

[28] OJ L183 of 20 May 2004, page 83.

3.4. EUROPEAN COURT OF JUSTICE

Transfer of air passengers' personal data to the US Bureau of Customs and Border Protection

The European Parliament decided to launch proceedings before the Court of Justice against the Council and the Commission for having adopted a legal framework (an adequacy decision and an international agreement) authorising the transfer of air passenger data to the US (Court cases C-317 and 318/04). The decision was based both on contentions that this legal framework does not adequately take the rights of the Parliament into account and that the arrangements do not provide for an adequate level of data protection. An earlier decision of Parliament to refer the proposed legal framework to the European Court of Justice for a legal opinion became obsolete as a result of the adoption of the two instruments.

3.5 EUROPEAN DATA PROTECTION SUPERVISOR

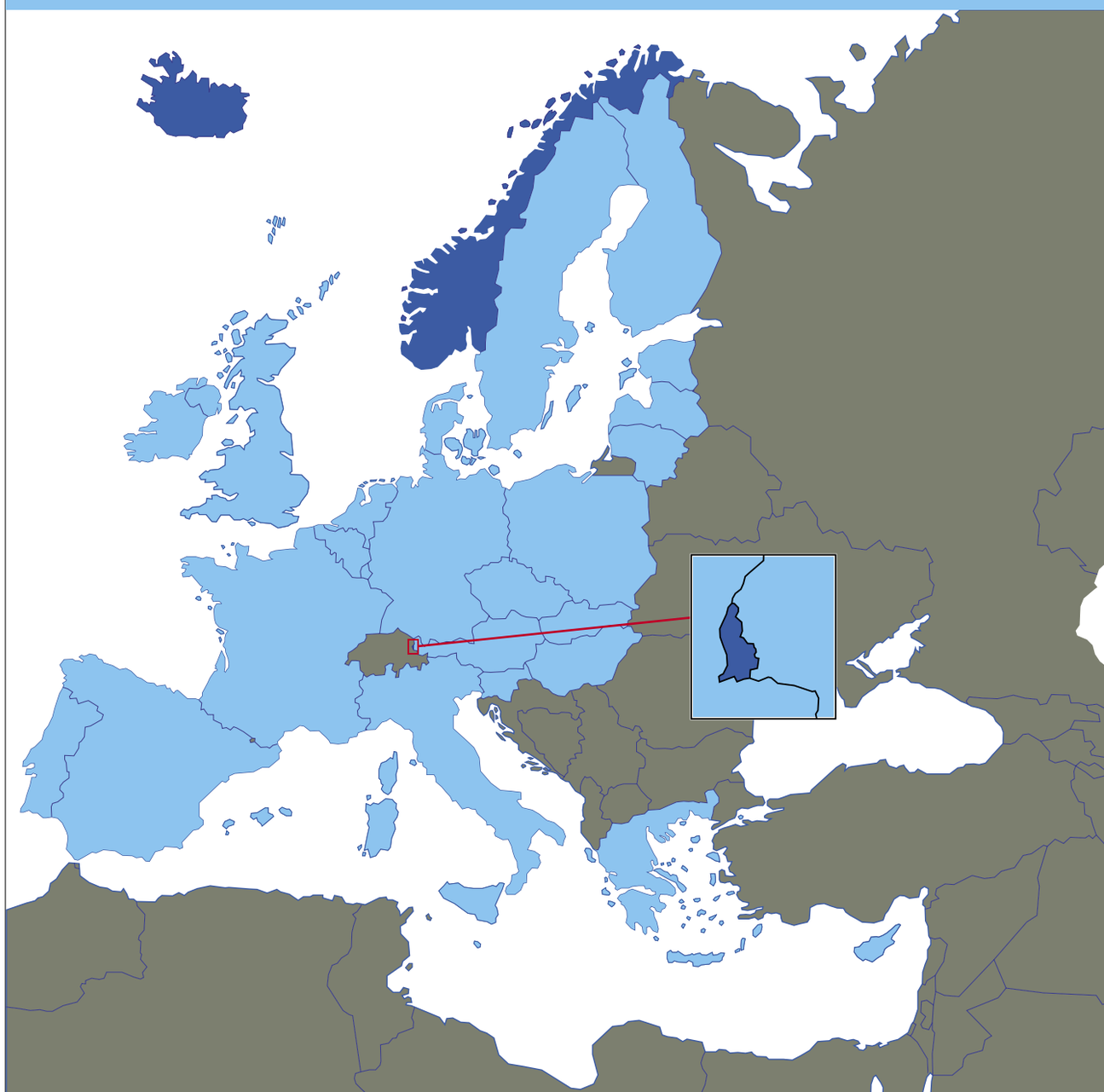
The European Data Protection Supervisor was appointed following the Decision No. 2004/55/EC of the European Parliament and of the Council of 22 December 2003 which came into effect on 17 January 2004. More information including the annual report 2004 can be found under http://www.edps.eu.int

3.6. EUROPEAN CONFERENCE

The annual Spring Conference of the Data Protection Authorities in the European Union, which in 2004 was organised in Rotterdam by the Dutch DPA, focused on effective supervision methods and arrangements. The three-day conference was opened on 22 April by Minister of Justice J.P.H. Donner, who called for further collaboration in supervising the enforcement of law and order in Europe within the third pillar, the policy area of the Ministries of Justice and Internal Affairs. The European privacy regulators have now intensified their collaboration in monitoring and advising on the areas of responsibility of the police and the Ministries of Justice.

Chapter Four

Main Developments in EEA Countries



Iceland

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

In 2004, a number of acts and administrative rules and regulations were passed. These are the most important ones:

1. Act on Insurance Contracts, No. 30/2004. – According to Article 82 paragraph 2 of this Act, an insurance company is not allowed, before or after the making of a contract on life, disease or accident insurance to wish for, obtain by some other means, receive, or make use of data on genetic characteristics of humans and the risk of them developing or getting diseases. A company is also not allowed to wish for research that is necessary so that such data can be obtained. This ban does not, however, apply to observations on the current or former health of the insurance applicant or other individuals. The Icelandic data protection authority, Persónuvernd, criticised this exception in its opinion on the parliamentary bill that later became the Act. However, Persónuvernd welcomed Article 82 paragraph 2 in other respects.

2. Regulation on Clinical Trials of Medicinal Products in Humans, No. 443/2004. – This regulation, passed by the minister of health in accordance with Articles 9 and 47 in the Medicinal Products Act, No. 93/1994, contains provisions on, amongst other things, the information that must be given to a research subject in a clinical trial of medicinal products, including the processing of personal data. Also, the regulation contains a provision on for how long data recorded in such a clinical trial shall be retained; in accordance with the international standard 'Good Clinical Practice' they shall be retained for 15 years after the final report on the study becomes available.

3. Rules on the Obligation to Notify or Obtain a Permit for the Processing of Personal Data, No. 698/2004. – These rules, passed by Persónuvernd in accordance with Act No. 77/2000, Articles 31 and 33, can be found in an English translation on the institution's website. The rules replace Rule No. 90/2001. The most significant change is that electronic surveillance, conducted for the purposes of security and property protection only, is no longer subject to the obligation to notify.

4. Rules on Electronic Surveillance in the Workplace, Schools, and in Other Areas Where a Limited Number of People Normally Traverses, No. 888/2004. – These Rules were passed by Persónuvernd in accordance with Act No. 77/2000, Article 37. They contain provisions on, amongst other things, when to resort to electronic surveillance, for how long data recorded in the course of such surveillance may be retained, the scanning of Internet use in the workplace, automatic recording of employees' driving information, surveillance for work supervision purposes, the duty of the one responsible for surveillance to give information to the data subjects, and the obligation of the one responsible for surveillance that leads to the processing of personal data, i.e. recording and passing rules on the surveillance.

B. Major case law

None to report.

C. Major specific issues

One of the main tasks that Persónuvernd undertook in 2004 was inspections. Formal administrative decisions were taken regarding inspections that began in 2002 and 2003, on the lawfulness and security of the processing of personal data in three biobanks and by the Road Traffic Directorate which processes, amongst other things, personal data regarding traffic accidents. No faults were found concerning the lawfulness of processing and only some minor ones concerning security.

In addition to these decisions, Persónuvernd delivered three opinions containing the conclusions of inspections regarding the lawfulness of processing of data on job applicants by employers. These inspections, which were started in 2003, were part of a pan-Nordic project on such processing. All the three parties that were inspected, a pharmaceutical company, a security company, and the customs department in Reykjavik, were given a number of recommendations on reforms in data processing.

Liechtenstein

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

The Data Protection Act (*Datenschutzgesetz* – DSG) was amended. The amendments concerned two main points. The first was to introduce a possibility of consulting the Register of Data Collections via Internet. Modern communication techniques can thus be used, and the administrative authority's burden is lightened correspondingly. The second extends certain transitional provisions. The new provision is that the authorities can continue processing personal profiles and sensitive personal data without there being a specific enabling provision in the legislation until 1 August 2007. This provision was needed because the requisite legislative amendments were not all in place by 1 August 2004.

The Data Protection Regulations (DSV) were also amended. Under the new section 28, the register no longer has to be published from time to time but can, as has been seen, be consulted via the Internet. A further amendment adapted section 5 (data transfers to other countries) to Directive 95/46/EC, taking over Article 25(2) from it, and the list of countries providing an adequate level of data protection in the Annex was adjusted.

Opinions on legislative instruments

In addition to the revisions of the DSG and DSV, the DPA was consulted on a further 21 pieces of draft legislation. The following are noteworthy:

- Regulation governing the health insurance card in connection with the European Health Insurance Card: this Regulation will be the basis for the Health Insurance Card and the Health Card. Initially, only administrative data will be processed. Subsequently health data may also be involved but only with the data subject's prior express consent. At the end of 2004 the Regulation was still at the draft stage.

- Communications Act: this Act transposes a series of Directives, including Directive 2002/58/EC on personal data and privacy in electronic communications. The Opinion was issued as part of the public consultation procedure. The draft will then be laid before the Landtag (Parliament).

- Treaty between Switzerland and Liechtenstein on the common use of fingerprint and DNA profile databases. This Treaty is to lay a proper legal basis for data transfers that have already been taking place in practice. In addition, the entire provisions of the Swiss DNA Profile Act will be taken over in Liechtenstein law. This is a further data protection measure, since it lays down clear legal rules.

- Treaty between the Government of Austria, the Swiss Federal Council and the Government of the Principality of Liechtenstein on mutual exchanges in asylum matters. At the end of 2004 this instrument was still at the draft stage but it lays a proper legal basis for data transfers in asylum matters.

B. Major case law

The reporting year saw the first report by the Data Protection Commission (DSK), supporting a recommendation made by the DSB to the local authorities and deciding that in future the local authorities could no longer publish construction permits without further ado. The provisions of the Data Protection Act must now be complied with. Up until then, the local authorities publicised all planning applications approved by them for the sake of transparency, using all sorts of media such as town hall notice boards, records of town council meetings, local TV stations, newsletters and websites. The result of the DSK's decision is that there is no legal basis for regular announcements of approved planning applications, without consent.

C. Major specific issues

In this second full reporting year, the focus was on the review of the central personnel administration (ZPV), a centrally managed database of the Liechtenstein national administration, for data protection compliance. This review looked into the access rights of official offices to individual data fields. The database, which is designed to simplify administrative procedures, chiefly contains the entire resident population with the full set of personal data. The core element is a national code number given to each person and corporate body. A comprehensive database, such as this, used to process personal profiles without a legal basis. The obligations of Article 8(7) of the data protection Directive 95/46/EC were not met. That Article requires the Member States to determine the conditions under which a national identification number or any other identifier of general application may be processed. At the beginning of 2004, the Government set up a working party to look into ZPV data protection issues. The group, on which data protection personnel are represented, agreed on an application procedure for those entitled to access data. Authorisations were issued based on criteria of the legal basis and proportionality. For various reasons it was not possible to complete the review by the end of 2004. The group is also looking into establishing a legal basis for the database. Similar questions arise in the local authorities, as they also store personal data on their population.

The DPA's website at www.sds.llv.li has been extended and updated on a more or less ongoing basis. Specific topics covered include data protection at school, data protection and e-Government, spam mail, video surveillance, precision of the Directives of the DPA on data release for inhabitants control purposes, DSB report for 2003, etc. The Register of data collections has not yet been uploaded to the DPA's website even though the legal basis has been established with the revision of the Data Protection Act.

Norway

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

Significant changes to privacy or data protection law

In 2004, the Data Inspectorate of Norway drew up proposals for amendments to the data protection regulations. The proposals aim to alleviate some aspects of the licensing obligation for research projects recommended by an ethical committee. The amendments came into force on 1 July 2005.

Significant changes to other laws affecting privacy or data protection

➔ The Currency Register Act

A new register was added to the Currency Register Act for control and investigation purposes in relation to currency exchange and currency movements in and out of the country.

The Data Inspectorate was of the opinion that the original proposal for full detailed registration of minor amounts and storage beyond ten years would be a needlessly extensive intrusion of individual privacy. In its debate on the draft legislation, the Storting, the Norwegian Parliament, opted for some reduction of the storage period and the level of detail for registration of minor amounts.

➔ The Working Environment Act

A statutory provision has been added to the Working Environment Act for regulations requiring that all employees be issued with special ID cards.

During the round of consultations, the Data Inspectorate had difficulty in seeing how such ID cards could help prevent social dumping and improve the working environment, as the initiative purported to do.

Furthermore, a legal authorisation has been introduced to give employers more control over employees, including the right to test them for intoxication under given conditions.

B. Major case law

None to report.

C. Major specific issues

Initiatives taken to assist organisations and agencies to meet their privacy obligations or otherwise enhance privacy.

Guidelines

The Data Inspectorate assisted in the formulation of three industrial norms: for an umbrella organisation for voluntary professional and industrial bodies, one industrial norm for the security of information in the health sector, and one for the processing of personal information in sports.

Consultations

Police methods

A public committee that assessed the police's need for using certain methods presented its work in the spring of 2004. One of the Data Inspectorate's senior advisers sat on the committee and raised some primary objections to the majority's proposals. In the Data Inspectorate's subsequent submission to the round of consultations, there was particular objection to the proposals for data reading and electronic room surveillance. Data reading is a highly intrusive method. By this method, non-communicated information can be subject to closer scrutiny by the police. This may be done, for example, by the police installing spyware on a computer used by the suspect. The software records every keystroke and also data that are subsequently deleted. The Data Inspectorate sees it as problematic that thoughts, associations and wishes that were never even intended for communication to others could be used to help prove someone's guilt.

A streamlined public sector

During the year, the Data Inspectorate was consulted on matters that raise key questions about the public sector's processing of personal information. Common to many of the initiatives is the desire to achieve a more cost-effective and user-oriented public administration, in line with the government's modernisation programme. Some of the proposed measures entail keeping large amounts of personal data in central databases, or establishing portals to enable the exchange of personal data between various administrative bodies. Examples of this are the Ministry of Modernisation's plans for a common public IT architecture and the establishment of a basic public authority database for the use of various administrative bodies. In addition, the Ministry of Health and Care's 'Norwegian Patient Register' and the Ministry of Education and Research's central register of pupils in relation to national tests have been established.

The Data Inspectorate's view is that strict mechanisms must be built in to reduce the possibility of personal data being needlessly distributed or abused in case of use of large databases.

In several cases, there has been virtually no evaluation with regard to privacy and security of information.

The reports advocate the principle of re-use and more efficient exploitation of various types of basis data across all public administration. A considerable part of the information exchanged will naturally consist of personal data. The fact that public administration will thereby gain easier access to ever increasing amounts of information about individual citizens, without being in direct contact with them, could, seen in isolation, contribute to a very efficient administration. On the other hand it could also contribute to an effective shift of power from individual citizens to the authorities.

Norwegian Patient Register

In 2004, the Ministry of Health and Social Affairs proposed to change the Norwegian Patient Register into a register linked to identity. This is something to which the Data Inspectorate is strongly opposed. During the round of consultations, the Data Inspectorate pointed out that a person-specific Norwegian Patient Register, with a centralised mapping of the health condition of individual Norwegian citizens and their use of hospitals from birth to death, would have a negative effect on the privacy of virtually everyone in Norway. The proposed Norwegian Patient Register is a key register. By abstracting a few items of information from it, it is possible to identify citizens in most other health registers – regardless of whether these registers are basically made anonymous or pseudonymous. If existing health registers are taken together in conjunction with the proposed patient register, information mapping becomes very comprehensive.

Increased focus on inspections

The Data Inspectorate decided in 2004 to organise some of its inspection activity into major projects. This method of organisation was chosen for sectors where it was considered important to add resources to undertake a particularly thorough, and thereby resource-demanding, mapping operation. Project-based inspections were made within the following areas:

- women's refuge centres
- electronic communications in the health sector
- the National Insurance Service
- medical research.

The Data Inspectorate appointed a project group which inspected 50 research projects during the spring of 2004. Inspections were made of 26 different health enterprises, teaching institutions, research institutions and manufacturers of pharmaceuticals. The project uncovered several issues that the Data Inspectorate considers serious. The Data Inspectorate found breaches of concessionary conditions, illegal storage of sensitive personal data, lack of internal control and lack of clearly defined areas of responsibility. A separate report in Norwegian has been drawn up, setting out findings and tendencies in connection with the project.

Fully automatic road toll stations

Even though no sensitive personal data are processed at the fully automatic road toll stations, the Data Inspectorate decided in the autumn of 2004 that the fully automatic road toll stations should be obliged to acquire a licence. The justification for being able to impose this requirement is that such processing will clearly violate important personal privacy interests. In the opinion of the Data Inspectorate, important personal privacy interests will clearly be violated if individuals cannot decide for themselves whether they want to leave traces of where they are travelling at any time along Norwegian roads. With the systems currently in use, road users are not offered solutions that leave them a real choice, whether it is information, availability, costs or functionality.

Testing for intoxicants

Securitas had established a system for testing its employees for intoxicants, based on their consent. However, the Data Inspectorate feels that the employer's right to govern and the consent of employees are not a sufficient legal basis for conducting intoxication tests. Although the Data Inspectorate must be careful when querying a granted consent, there is no doubt that many employees feel under an obligation to consent to this type of intrusion. The consequence of refusing to agree to test for intoxicants could easily be that they would be denied a job.

Chapter Five

Members and Observers of the Article 29 Data Protection Working Party

MEMBERS IN 2004

AUSTRIA Frau Dr Waltraut KOTSCHY Österreichische Datenschutzkommission	**BELGIUM** Monsieur Paul THOMAS Président Commission de la Protection de la Vie privée
CYPRUS* Ms Goulla FRANGOU Commissioner for Personal Data Protection	**CZECH REPUBLIC*** Dr Karel NEUWIRT President The Office for Personal Data Protection
DENMARK Ms Janni CHRISTOFFERSEN Director Datatilsynet	**ESTONIA*** Mr Urmas KUKK Director General Estonian Data Protection Inspectorate
FINLAND Mr Reijo AARNIO Data Protection Ombudsman Office of the Data Protection Ombudsman Ministry of Justice	**FRANCE** Ms Anne DEBET Chef de la division des Affaires européennes, internationales et prospective Commission Nationale de l'Informatique et des Libertés (CNIL)
GERMANY Herr Peter SCHAAR Chairman Der Bundesbeauftragte für den Datenschutz	**GREECE** Mr Nikolaos FRANGAKIS Hellenic Data Protection Authority
HUNGARY* Mr Attila PETERFALVI Parliamentary Commissioner Office of the Parliamentary Commissioner for Data Protection and Freedom of Information	**IRELAND** Mr Joe MEADE Data Protection Commissioner Irish Life Centre
ITALY Prof. Stefano RODOTA Président Garante per la Protezione dei Dati personali	**LATVIA*** Ms Signe PLUMINA Director of the Data State Inspection
LITHUANIA* Ms Ona JAKSTAITE Director State Data Protection Inspectorate	**LUXEMBOURG** M. Gérard LOMMEL Président Commission nationale pour la Protection des Données
MALTA* Mr Paul MIFSUD-CREMONA Commissioner for Data Protection Office of the Commissioner for Data Protection	**THE NETHERLANDS** Mr Ulco VAN DE POL College Bescherming Persoonsgegevens (CBP)

* as of 1 May 2004

POLAND* Ms Ewa KULESZA Inspector General The Bureau of General Inspector for Personal Data Protection	**PORTUGAL** Mr Luís DA SILVEIRA Président Comissão Nacional de Protecção de Dados
SLOVAKIA* Mr Pavol HUSAR The Office for the Protection of Personal Data	**SLOVENIA*** Mr Jernej ROVSEK Deputy Ombudsman Republic of Slovenia Human Rights Ombudsman
SPAIN Mr José Luis PIÑAR MAÑAS Vice chair Director Agencia de Protección de Datos	**SWEDEN** Mr Göran GRÄSLUND Director General Datainspektionen
THE UNITED KINGDOM Mr Richard THOMAS Information Commissioner The Office of the Information Commissioner Executive Department	**EUROPEAN DATA PROTECTION SUPERVISOR** Mr Peter HUSTINX European Data Protection Supervisor

* as of 1 May 2004

OBSERVERS IN 2004

ICELAND Ms Sigrun JOHANNESDOTTIR Director Icelandic Data Protection Agency	**NORWAY** Mr Georg APENES Director General Datatilsynet The Data Inspectorate
LIECHTENSTEIN Herr Dr Philipp MITTELBERGER Data Protection Commissioner of the Principality of Liechtenstein	

MEMBERS AS OF 25 NOVEMBER 2005

AUSTRIA Frau Dr Waltraut KOTSCHY Österreichische Datenschutzkommission Ballhausplatz 1 – AT - 1014 Wien Tel: +43 1 531 152679; +43 1 531 152525 Fax: +43 1 531 152690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	**BELGIUM** Monsieur Michel PARISSE Président Commission de la Protection de la Vie privée Rue Haute, 139– BE - 1000 Brussels Tel: +32 2 213 8540 Fax: +32 2 213 8565 E-mail: commission@privacycommission.be Website: http://www.privacy.fgov.be
CYPRUS Ms Goulla FRANGOU Commissioner for Personal Data Protection 40, Themistokli Dervi str. Natassa Court, 3rd floor – CY - 1066 Nicosia or P.O. Box 23378 – CY - 1682 Nicosia Tel: +357 22 818 456 Fax: +357 22 304 565 E-mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy	**CZECH REPUBLIC** Mr Igor NEMEC President Office for Personal Data Protection Pplk. Sochora 27 – CZ - 170 00 Praha 7 Tel: +420 234 665 281 Fax: +420 234 665 501 E-mail: info@uoou.cz Website: http://www.uoou.cz/
DENMARK Ms Janni CHRISTOFFERSEN Director Datatilsynet Borgergade 28, 5th floor – DK - 1300 Koebenhavn V Tel: +45 33 193236 Fax: +45 33 193218 E-mail: dt@datatilsynet.dk Website :http://www.datatilsynet.dk	**ESTONIA** Mr Urmas KUKK Director General Estonian Data Protection Inspectorate Väike - Ameerika 19 – EE - 10129 Tallinn Tel: +372 6274 135 Fax: +372 6274 135; Fax: +372 6274 137 E-mail: urmas.kukk@dp.gov.ee; info@dp.gov.ee Website: http://www.dp.gov.ee
FINLAND Mr Reijo AARNIO Data Protection Ombudsman Office of the Data Protection Ombudsman P.O. Box 315 – FI - 00181 Helsinki Tel: +358 10 36 66700 Fax: +358 10 36 66735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi	**FRANCE** Mr Georges de La LOYERE Commissaire en charge du secteur international Commission Nationale de l'Informatique et des Libertés (CNIL) Rue Saint Guillaume, 21– FR - 75340 Paris Cedex 7 Tel: +33 1 53 73 22 31; +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-mail: laloyere@cnil.fr Website: http://www.cnil.fr

GERMANY Herr Peter SCHAAR Chairman Der Bundesbeauftragte für den Datenschutz Herr Peter Schaar Husarenstraße 30 – DE - 53117 Bonn Tel: +49 228 81995 0 Fax: +49 228 81995 550 E-mail: peter.schaar@bfd.bund.de Website: http://www.bfd.bund.de	**GREECE** Mr Nikolaos FRANGAKIS Lawyer Hellenic Data Protection Authority Kifisias Av. 1-3, PC 115 23 Ampelokipi – GR - Athens Tel: +30 210 6475 601; +30 210 3352 602 Fax: +30 1 3352 617 E-mail: sofralaw@otenet.gr Website: http://www.dpa.gr
HUNGARY Dr Attila PETERFALVI Parliamentary Commissioner Office of Parliamentary Commissioners Nador u. 22 – HU - 1051 Budapest Tel: +36 1 475 7186; +36 1 475 7100 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Website: http://abiweb.obh.hu	**IRELAND** Mr Billy HAWKES, Data Protection Commissioner Irish Life Centre, Block 6 Lower Abbey Street– IE - Dublin 1 Tel: +353 1 8748544 Fax: +353 1 8745405 E-mail: info@dataprotection.ie Website: www.dataprotection.ie
ITALY Professor Francesco PIZZETTI Président Garante per la protezione dei dati personali Piazza di Monte Citorio, 121– IT - 00186 Roma Tel: +39 06 69677403 Fax: +39 06 06 69677405 E-mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it	**LATVIA** Ms Signe PLUMINA Director Data State Inspectorate Kr. Barona Street 5-4 – LV - 1050 Riga Tel: +371 722 31 31 Fax: +371 722 35 56 E-mail: info@dvi.gov.lv Website: http://www.dvi.gov.lv
LITHUANIA Ms Ona JAKSTAITE Director State Data Protection Inspectorate Gedimino Ave 27/2 – LT - 2600 Vilnius Tel: +370 5 279 1445 Fax: +370 5 261 9494 E-mail: ada@ada.lt Website: http://www.ada.lt	**LUXEMBOURG** M. Gérard LOMMEL Président Commission nationale pour la Protection des Données 68, rue de Luxembourg– LU - 4100 Esch-sur-Alzette Tel: +352 261 06020 Fax: +352 261 06029 E-mail: info@cnpd.lu Website: http://www.cnpd.lu
MALTA Mr Paul MIFSUD CREMONA Data Protection Commissioner 2, Airways House High Street – MT - SLM 16 Sliema Tel: +356 2328 7100 Fax: +356 2328 7198 E-mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt	**THE NETHERLANDS** Mr Jacob KOHNSTAMM College Bescherming Persoonsgegevens (CBP) Prins Clauslaan 20 Postbus 93374 – NL - 2509 AJ 's-Gravenhage Tel: +31 70 381.13.00 Fax: +31 70 381.1301 E-mail: info@cbpweb.nl Website: http://www.cbpweb.nl; www.DutchDPA.nl

POLAND
Ms Dr Ewa KULESZA
Inspector General for Personal Data Protection
Bureau of the Inspector General for Personal Data Protection
ul. Stawki 2 – PL - 00193 Warsaw
Tel: +48 22 860 70 81; +48 22 860 73 12
Fax: +48 22 860 70 90
E-mail: sekretariat@giodo.gov.pl; dp@giodo.gov.pl
Website: http://www.giodo.gov.pl

PORTUGAL
Mr Luís DA SILVEIRA
Président
Comissão Nacional de Protecção de Dados
Rua de São Bento, 148, 3º
PT - 1 200-821 Lisboa Codex
Tel: +351 21 392 84 00
Fax:+351 21 397 68 32
E-mail: geral@cnpd.pt
Website: http://www.cnpd.pt

SLOVAKIA
Mr Gyula VESZELEI
President
Office for the Personal Data Protection of Slovakia
Odborarska namestie 3 – SK - 81760 Bratislava 15
Tel: +421 2 5023 9418
Fax: +421 2 5023 9441
E-mail: statny.dozor@pdp.gov.sk: gyula.veszelei@pdp.gov.sk
Website: http://www.pdp.gov.sk

SLOVENIA
Mr Jože BOGATAJ
The Acting Chief Inspector for Personal Data Protection
Ministry of Justice of the Republic of Slovenia
Inspectorate for Personal Data Protection of the Republic of Slovenia
Tivolska 50 – SI - 1000 Ljubljana
Tel: +386 1 478 5260
Fax: +386 1 478 5344
E-mail: joze.bogataj@gov.si
Website: http://www.mp.gov.si

SPAIN
Mr José Luis PIÑAR MAÑAS
Vice Chair
Director
Spanish Data Protection Agency
C/ Sagasta, 22– ES - 28004 Madrid
Tel: +34 91 399 6219/20
Fax: +34 91 447 1092
E-mail: director@agpd.es
Website: http://www.agpd.es

SWEDEN
Mr Göran GRÄSLUND
Director General
Datainspektionen
Fleminggatan, 14
9th Floor
Box 8114 – SE - 104 20 Stockholm
Tel: +46 8 657.61.00; +46 8 657.61.57
Fax: +46 8 650.86.13; +46 8 652.86.52
E-mail: datainspektionen@datainspektionen.se; Goran.graslund@datainspektionen.se
Website: http://www.datainspektionen.se

THE UNITED KINGDOM
Mr Richard THOMAS
Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane – GB - SK9 5AF Wilmslow
Tel: +44 1625 545700 Fax: +44 1625 524 510
E-mail: pdq@ico.gsi.gov.uk; mail@ico.gsi.gov.uk
Website: http://www.informationcommissioner.gov.uk

EUROPEAN DATA PROTECTION SUPERVISOR
Mr Peter HUSTINX
European Data Protection Supervisor
Postal address:
Rue Wiertz 60– BE - 1047 Brussels
Office:
Rue Montoyer 63, 6th floor– BE - 1047 Brussels
Tel: + 32 2 283 1900
Fax: +32 2 283 1950
E-mail: edps@edps.eu.int
Website: http://www.edps.eu.int

OBSERVERS AS OF 25 NOVEMBER 2005

ICELAND
Ms Sigrun JOHANNESDOTTIR
Director
Icelandic Data Protection Authority
Raudararstigur 10 – IS - 105 Reykjavik
Tel: +354 560.90.10; +354/510 9600
Fax: +354 510 9606
E-mail: postur@personuvernd.is
Website: http ://www.personuvernd.is

NORWAY
Mr Georg APENES
Director General
Datatilsynet
The Data Inspectorate
P.B. 8177 Dep – NO - 0034 Oslo
Tel: +47 22 396900
Fax: +47 22 422350
E-mail: postkasse@datatilsynet.no
Website: http://www.datatilsynet.no

LIECHTENSTEIN
Herr Dr Philipp MITTELBERGER
Data Protection Commissioner of the Principality of Liechtenstein
Aeulestrasse 51– LI - 9490 Vaduz
Tel: +423 236 6090/ 91
Fax: +423 236 6099
E-mail: info@sds.llv.li
Website: http://www.sds.llv.li; http://www.liechtenstein.li

BULGARIA
Mr Ivo STEFANOV
Commission for Personal Data Protection (CPDP)
1 Bvld Dondukov – BG - 1000 Sofia
Tel: +359 2 940 2046
E-mail: kzld@government.bg

ROMANIA
Ms Georgeta BASARABESCU
President
National Supervisory Authority for Personal Data Processing
Eugeniu Carada Street, no. 3, Sector 3 – RO - Bucharest
Tel: +40 21 312 4934
Fax: +40 21 312 7102
E-mail: basarabescu@avp.ro

SECRETARIAT OF THE ARTICLE 29 WORKING PARTY
Mr Philippe RENAUDIERE
Head of unit
Data Protection Unit
Directorate-General Justice, Freedom and Security
European Commission
Office: LX46 01/43 – BE - 1049 Brussels
Tel: +32 2 296 8750
Fax: +32 2 299 8094
E-mail: Philippe.Renaudiere@cec.eu.int
Website: http://europa.eu.int/comm/justice_home/fsj/privacy/