European Commission
Justice

Thirteenth Annual Report
of the Article 29 Working Party on
Data Protection

1830-6446

Thirteenth Annual Report

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

Covering the year 2009

Adopted on 14 July 2010

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission,
Directorate General Justice, Belgium, Office No LX-46 01/190.

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

TABLE OF CONTENTS

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

2009 saw new technologies evolve at a frenetic pace, in a world without boundaries. Our legal framework and practices need to adapt to these profound transformations, while also maintaining a high level of data protection.

At the 31st International Conference of Data Protection and Privacy Commissioners (Madrid, November 2009), we established the possible basis for the global regulation of data protection with the adoption of a resolution aimed at establishing international standards for the protection of privacy and personal data. This represents a historic step as data protection authorities managed to draw up, for the first time at a global level, a body of common principles adapted to the latest technological developments.

A reflection about the organic and legal consequences of these choices is necessary and a major awareness-raising exercise targeting public authorities must be promptly undertaken to ensure that they take steps to implement a legally binding international instrument.

At the same time, a reflection on the adaptation of existing tools has been commenced at European level. Among the initiatives launched in 2009, I would like to mention more particularly the initiative of the European Commission, which, at the instigation of its Vice-President, Jacques Barrot, and WP29, organised a large public consultation aimed at obtaining contributions regarding the new challenges in the field of data protection and improvements to the legal framework for data protection within the European Union.

The Article 29 Working Party and the Working Party on Police and Justice have applied their experience and expertise to issue a major opinion both at European level and for data protection in general, particularly taking into account the impact of the entry into force of the Lisbon Treaty on 1 December. This opinion sets out proposals for improving existing tools and practices. Among others, we cite the wish to develop practical measures for individuals, particularly by improving the clarity of their rights and implementing concrete means of action to exercise them. It is also necessary to raise corporate data protection to the level of common, shared ethical values and to strengthen the concrete efficiency of the actions undertaken by data controllers to demonstrate their compliance with the applicable regulations.

Moreover, there has been reflection on the independence and evolution of the role and powers of data protection authorities that perform a watchdog role by alerting public authorities or, more broadly, the general public, as soon as possible to issues that could quickly become major problems for society.

I had the opportunity to voice my concerns in the end-of-office letter I sent to my European counterparts in February 2010. I have always considered - and continue to do so - that WP29 must play a leading role in the European and international arenas in the field of data and privacy protection. However, I have observed that, in its current state of operation, WP29 has become severely handicapped by its lack of independent financial resources.

Increasing the resources available to WP29 would make it possible to organise more hearings, bring in more specialists in order to be able to respond to the latest technological developments and, more generally, take the necessary actions to make its voice heard on key issues. The granting of an independent budget to WP29 and the establishment of a dedicated secretariat would ensure the effectiveness, visibility and independence – and therefore the credibility – of WP29 in the coming years.

The work of WP29 is also being hindered by a severe lack of operating resources, in particular premises. Moreover, it is difficult to ensure appropriate interpreting services for each meeting to enable all the national experts to participate in the work of WP29. In addition, our working party needs more efficient communication tools, notably a dedicated website. Improved communication tools would certainly increase the visibility of the work and actions carried out.

Thus, as a matter of urgency, data protection authorities and the Article 29 Working Party must be granted the human and financial resources they need to effectively perform their work.

Alex Türk

Chapter One

ISSUES ADDRESSED BY THE ARTICLE 29 DATA PROTECTION WORKING PARTY[1]

[1] All documents adopted by the Art. 29 Data Protection Working Party can be found under http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

1.1. TRANSFER OF DATA TO THIRD COUNTRIES

1.1.1. Passenger Data / PNR

Opinion 8/2009 (WP 167) on the protection of passenger data collected and processed by duty free shops at airports and ports

Community law allows for the exemption of excise duties for purchases made in duty free shops at airports and ports by passengers. Such purchases, however, are subject to certain conditions. To fulfil these conditions, most shops in EU Member States collect and process data including passenger data when items are purchased.

However, the practice with regard to the processing and collection of such passenger data across Europe varies considerably in duty free shops. Passengers are at no point informed that their data – including their personal data, the purpose of the collection, their rights, and the use of these details by public bodies if such data is transferred to them – is being collected.

In accordance with Article 30 of Directive 95/46/EC, the European Commission has asked the Art. 29 WP to look into this matter and review the current practice in EU Member States with regard to data protection questions and, if necessary, make recommendations on a uniform application of the general data protection principles to be observed in duty free shops at airports and ports.

This opinion analyses the legal and practical issues surrounding the collection and processing of passenger data in duty free shops and aims to give guidance to shopkeepers and customs authorities charged with supervising the implementation of Community law with a view to coming to a more harmonised application of existing provisions.

1.1.2. Standard Contractual Clauses

Opinion 3/2009 (WP 161) on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor)

For several years, companies and Data Protection Authorities (DPAs) have been working with the standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46 (data controller to data processor 2002/16/EC) approved by the European Commission on 27 December 2001[2].

Although the standard contractual clauses 2002/16/EC provide a solid base for the transfer of personal data, the calls for an "update" of this contract have grown louder every year. The main reason to consider an "update" of the standard contractual clauses 2002/16/EC is the advent of "global outsourcing". As more and more companies not only transfer their data to a processor but to "sub-processors" and sometimes transfer data to subsequent "sub-sub-processors", the standard contractual clauses 2002/16/EC do not provide a means to deal with these complex onward transfers. Therefore, the European Commission considers it necessary to modify the standard contractual clauses 2002/16/EC to make a contract better equipped for current business arrangements by adopting a new Decision based on Article 26(4) of Directive 95/46/EC.

1.1.3. World Anti-Doping Agency (WADA)

Second opinion 4/2009 (WP 162) on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organisations

[2] OJ L 6, 10.12002, p.52. See Opinion of the Working Party no. 7/2001, WP 47) available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp47en.pdf

In its first opinion on this topic[3], the Working Party examined the compatibility of the draft International Standard for the Protection of Privacy and Personal Information (the Privacy Standard or the Standard) with the minimum level of protection required by European data protection regulations. Although it expressed its support for a number of aspects of the Standard, including a reference to Directive 95/46/EC, it did not conclude that it was compatible with the minimum level of protection offered by the Directive, and made certain recommendations.

The draft standard has since been modified and has been in force since 1 January 2009. The World Anti-Doping Agency (WADA) has provided additional information in response to the Working Party's previous requests for clarification. The Working Party is happy that some of its remarks have been integrated in the Privacy Standard[4]. It regrets, however, that its other remarks have not been taken into account (see point 3.2. below).

The 2005 UNESCO International Convention against Doping in Sport, which has been ratified by 25 of the 27 EU Member States, was concluded in order to endorse the work of WADA at international level. The Convention does not alter the rights and obligations of the signatories in relation to other agreements previously entered into (Article 6). It encourages cooperation between States in appropriate circumstances, and always subject to domestic law. According to EU law, any provisions in an international agreement which are incompatible with EU law are subordinate to the latter. The UNESCO Convention does not make any specific reference either to fundamental rights in general or data protection rights in particular.

The Working Party cannot confine its remarks only to the Privacy Standard. As the Privacy Standard contains numerous references to the WADA Code and to the ADAMS database (see 2.2.), it is necessary to examine it in the broader context of its application. That is why, after recalling the main features of the system developed by WADA (point 2), the opinion refers in more detail to the following matters: whereabouts (3.1.), un-integrated remarks from the first opinion (3.2.), grounds for processing (3.3.), the transfer of data to the ADAMS database in Canada and to other countries outside the EU (3.4.), retention periods (3.5.) and sanctions (3.6.).

Controllers in the EU, such as national anti-doping organisations (NADOs), national and international sports federations and Olympic Committees, can assess some of the legal boundaries that exist for processing athletes´ (and other data subjects') personal data. The Working Party emphasises that controllers in the EU are responsible for processing personal data in compliance with EU and domestic law and must, therefore, disregard the World Anti-Doping Code and International Standards insofar as they contradict them. The Working Party recommends that these controllers seek legal advice.

1.1.4. Adequacy

Opinion 6/2009 (WP 165) on the level of protection of personal data in Israel

On 12 July 2007, the Israeli Mission to the European Union made a request to the Commission to launch the procedure to declare Israel as a country that ensures an adequate level of protection for the purposes provided for in Articles 25 and 26 of the Directive.

In order to examine Israel's adequacy, the Commission made a request to the Centre de Recherches Informatique et Droit (hereinafter "CRID") of Namur University to produce an extensive report that analysed the extent to which the Israeli regulatory system fulfilled the requirements for the application of the personal data protection regulations set out in the Working Document "Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection Directive", adopted by the Working Party set up under Article 29 of the Directive on 24 July 1998 (document WP12).

[3] Opinion 3/2008 of 1 August 2008 on the World Anti-Doping Code Draft International Standard for the Protection of Privacy (WP 156) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp156_en.pdf

[4] The modified definition of "processing", of "sensitive data" (which no longer includes political opinions, religious or philosophical beliefs and trade-union membership, whose relevance in the fight against doping was questioned by the Working Party (3.2.)) and the clarification provided under 6.2. The Working Party has also observed that article 6 has been rewritten and in addition to consent (henceforth informed), it now also provides that "Personal information" shall be processed "where expressly permitted by law". It has also noted other modifications in line with its remarks, including the drafting of the comment to article 9.2, the term "plainly vexatious" being deleted under 11.2. with regard to the exercise of the right of access, and Participants' rights to initiate a complaint with an international anti-doping organisation now being provided for in article 11.5.

The aforementioned report, together with the preliminary response to it from the Israeli authorities, was discussed by the Safe Harbour Subgroup during a meeting held on 18 March 2009. At that meeting, the Subgroup submitted a proposal to the Working Party, with a view to obtaining an opinion, that its President should send a letter to the Israeli authorities which, while positively assessing the existing data protection scheme in Israel, would highlight those issues that required further clarification.

On 2 September 2009, the Israeli authorities sent an extensive report through the Israeli Law, Information and Technology Authority (hereinafter "ILITA") to the Working Party, in which they responded to the issues raised in the above-mentioned letter. This report has been analysed by the members of the Subgroup, and was also the subject of a hearing of the aforementioned authorities, which was held on 16 September 2009. During that meeting, the members of the Subgroup asked the Israeli authorities, represented by the Head of ILITA and the Head of its Legal Department, to clarify those issues that, following the earlier discussion of the report sent to the Subgroup, still needed further clarification.

The Subgroup informed the Working Party during its meeting held on 12 and 13 October 2009 of the conclusions reached at the meeting of 16 September and proposed the adoption of the present Opinion, under the terms contained herein. The proposal was approved by the Working Party at the aforementioned meeting.

Opinion 7/2009 (WP 166) on the level of protection of personal data in the Principality of Andorra

On 21 May 2008, the Ambassador of Andorra to the European Union made a request to the Commission to launch the procedure to declare Andorra as a country that offers an adequate level of protection within the meaning of article 25(6) of Directive 95/46/EC, on Personal Data Protection.

In order to proceed with the study of the adequacy of Andorra, the Commission requested a report from the Centre de Recherches Informatique et Droit (CRID) of the University of Namur, which issued an extensive report that analysed to what extent the Andorran regulatory system met the requirements of substantive legislation and implemented mechanisms applicable to the regulations for the protection of personal data established in the Working Document "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", adopted by the Working Party created by article 29 of the Directive on 24 July 1998 (document WP12).

This report was discussed in the meeting of the Safe Harbour Subgroup held on 18 March 2009. In this meeting, the Subgroup requested an opinion from the Working Party regarding a letter sent by its Chairman to the Andorran authorities, in which, after positively assessing the existing data protection regime in Andorra, those authorities were informed of the matters that required further clarification.

On 31 July 2009, the Andorran authorities, via the Andorran Data Protection Agency (APDA), sent an extensive report to the Article 29 Working Party in which they responded to the questions posed in the aforementioned letter. This report was analysed by the Subgroup, and was also the subject of an interview with the relevant authorities, held on 16 September 2009, during which the members of the Subgroup asked the Andorran authorities, represented by the Director of the APDA, its Inspection Manager and the Manager of Legal Consultancy, to clarify those matters which, after the previous discussion of the report sent by the same to the Subgroup, were still considered to require clarification.

The Subgroup informed the Working Party, during the meeting of the same held on 12 and 13 October 2009, regarding the conclusions reached in that meeting and proposed the adoption of this Opinion to the Working Party under the terms contained herein, with the proposal then being approved by the Working Party during the meeting.

1.1.5. Pre-trial discovery

Working document 1/2009 (WP 158) on pre-trial discovery for cross border civil litigation

This working document provides guidance to data controllers subject to EU Law in dealing with requests to transfer personal data to another jurisdiction for use in civil litigation. The Working Party has issued this document to address its concern that there are different applications of Directive 95/46, which partly result from the variety of approaches to civil litigation across the Member States.

In the first section of this document, the Working Party briefly sets out the differences in attitudes to litigation and in particular the pre-trial discovery process between common law jurisdictions such as the United States and the United Kingdom and civil code jurisdictions.

The document goes on to set out guidelines for EU data controllers when trying to reconcile the demands of the litigation process in a foreign jurisdiction with the data protection obligations of Directive 95/46.

1.2. ELECTRONIC COMMUNICATIONS, INTERNET AND NEW TECHNOLOGIES

Opinion 1/2009 (WP 159) on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)

On 13 November 2007, the Commission adopted a Proposal for a Directive ("the Proposal") amending Directive 2002/58/EC (e-Privacy Directive) concerning the processing of personal data and the protection of privacy in the electronic **communications sector** and Directive 2002/21/EC (Framework Directive). The proposal was eventually adopted by the European Parliament and the Council on 25 November 2009.

The Working Party had already adopted two Opinions on the proposals amending the EU's regulatory framework for electronic communications networks and services (Opinion 8/2006 adopted on 26 September 2006[5] and Opinion 2/2008 adopted on 15 May 2008[6]).

Though the Working Party is pleased that some of its previous recommendations were taken into account, it wishes to underline some essential concerns related to the issues raised after the first reading in the Parliament and in the Council.

Opinion 5/2009 (WP 163) on online social networking

This Opinion focuses on how the operation of social networking sites (SNS) can meet the requirements of EU data protection legislation. It is mainly intended to provide guidance to SNS providers on the measures that need to be in place to ensure compliance with EU law.

The Opinion notes that SNS providers and, in many cases, third party application providers, are data controllers with corresponding responsibilities towards SNS users. The Opinion outlines how many users operate within a purely personal sphere, contacting people as part of the management of their personal, family or household affairs. In such cases, the Opinion deems that the 'household exemption' applies and the regulations governing data controllers do not apply. The Opinion also specifies circumstances whereby the activities of a user of an SNS are not covered by the 'household exemption'. The dissemination and use of information available on SNS for other secondary, unintended purposes is of key concern to the Article 29 Working Party. Robust security and privacy-friendly default settings are advocated throughout the Opinion as the ideal starting point with regard to all services on offer. Access to profile information emerges as a key area of concern. Topics such as the processing of sensitive data and images, advertising and direct marketing on SNS and data retention issues are also addressed.

Key recommendations focus on the obligations of SNS providers to conform with the Data Protection Directive and to uphold and strengthen the rights of users. Of paramount importance, SNS providers should inform

[5] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

[6] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf

users of their identity from the outset and outline all the different purposes for which they process personal data. Particular care should be taken by SNS providers with regard to processing the personal data of minors. The Opinion recommends that users should only upload pictures or information about other individuals, with the individual's consent and considers that SNS also have a duty to advise users regarding the privacy rights of others.

1.3. PERSONAL DATA

Opinion 2/2009 (WP160) on the protection of children's personal data (General Guidelines and the special case of schools)

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

This document should be seen in the context of the general initiative of the European Commission described in its communication "Towards an EU strategy on the Rights of the Child". In contributing to this general purpose, it aims to strengthen the fundamental right of children to personal data protection. This subject is not entirely new to the Art 29 Working Party, which has already adopted several opinions related to this issue. Its opinions on the FEDMA code of conduct (Opinion 3/2003), on geolocation (Opinion 5/2005) and on Visa and Biometrics (Opinion 3/2007) include certain principles or recommendations concerning children's data protection.

The aim of this document is to consolidate this issue in a structured way, defining the applicable fundamental principles (Part II) and illustrating them by reference to school data (Part III).

The area of school data was chosen because it is one of the more important sectors of children's lives, and comprises a significant part of their daily activities. The importance of this area is due also to the sensitive nature of much of the data processed in educational institutions.

The Future of Privacy: Joint contribution (WP 168) to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data

On 9 July 2009, the Commission launched a Consultation on the revision of the legal framework for the fundamental right to the protection of personal data. In its consultation, the Commission asked for views on the new challenges to personal data protection, in particular in the light of new technologies and globalisation. It wants to have input on the questions of whether the current legal framework meets these challenges and what future action would be needed to address the identified challenges. This opinion contains the joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to this consultation.

The central message of this contribution is that the main principles of data protection, as enshrined in Directive 95/45/EC, are still valid. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. On the contrary, it is useful to use the opportunity in order to:

- Clarify the application of some key rules and principles of data protection (such as consent and transparency).
- Bring the framework up to date by introducing additional principles (such as 'privacy by design' and 'accountability').
- Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
- Incorporate the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

1.4. ACCOUNTING, AUDITING & FINANCIAL MATTERS

Contribution of the Article 29 Working Party (WP 164) to the public consultation of DG MARKT on the report of the Expert Group on Credit Histories

The Article 29 Working Party welcomes the opportunity given by the European Commission to comment on the report of the Expert Group on Credit Histories (EGCH) which is open for public consultation. The Article 29 Working Party notes that the EGCH has been given a mandate by the European Commission to identify solutions that optimise circulation of consumers' credit data within the EU. The Working Party acknowledges that, in the course of carrying out this mandate, the EGCH has also discussed the right to privacy and other consumer protection considerations. In this respect, the Working Party notes and welcomes that the EGCH has decided not to recommend the establishment of a central EU credit data system nor alignment of all Member States on one existing or new credit data model.

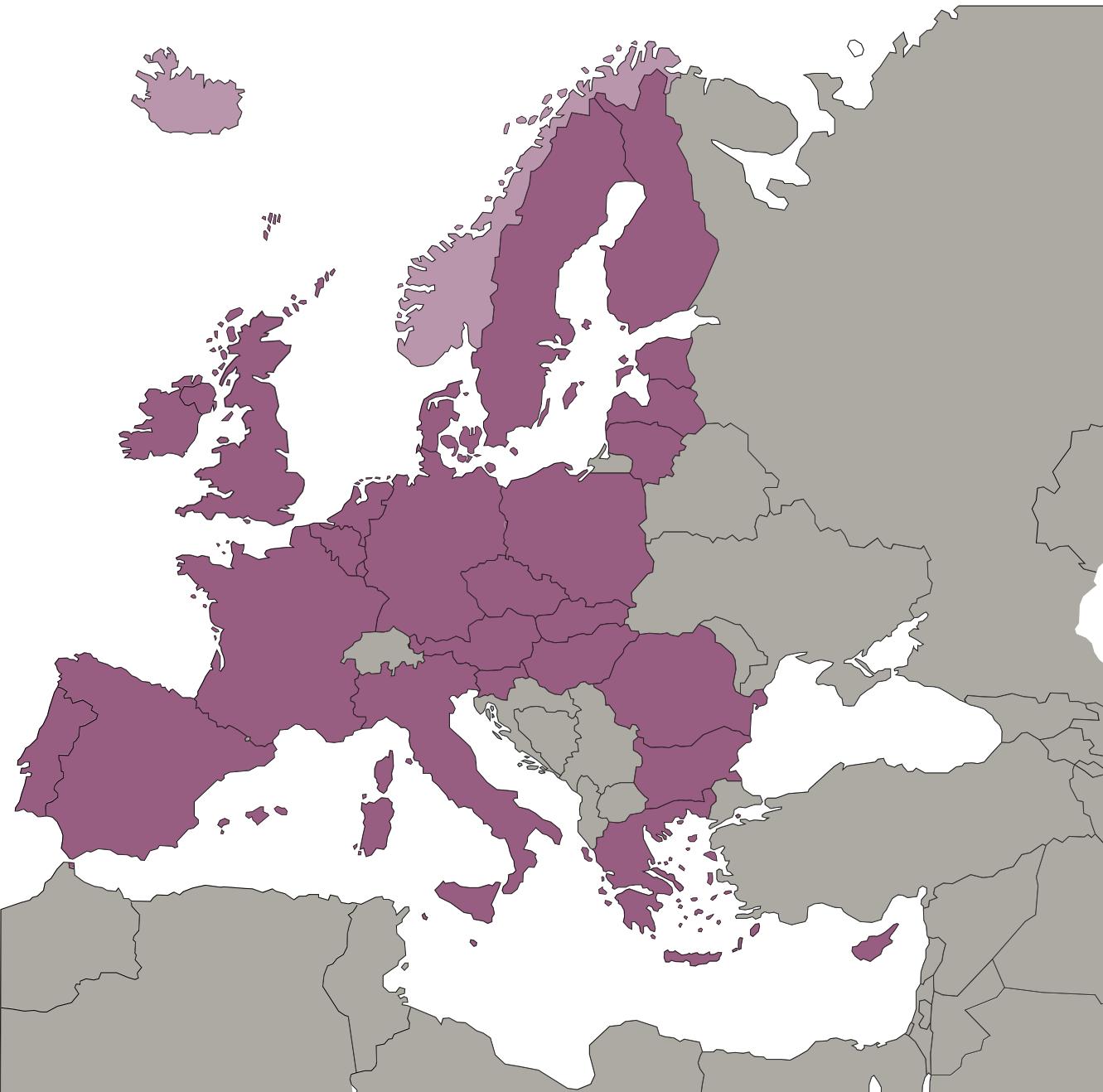
The Article 29 Working Party pointed out in its opinion that the approach taken by the EU/EEA data protection authorities to such matters is based on the Data Protection Directive (Directive 95/46/EC) and the different legislative frameworks in each Member State transposing that Directive. The EGCH report addresses important matters, such as harmonisation of regulations, roundtable discussions and cooperation between data protection authorities. The Article 29 Working Party, therefore, urges the Expert Group to adopt a firm and clear position and to obtain formal commitments from all parties involved on the matters which require regulatory measures.

The recommendations made by the Expert Group in the report mainly reflect the concerns of the financial sector, since the majority of the members of the Expert Group represent financial institutions. The members of the Article 29 Working Party, therefore, believe that this contribution and the reactions of consumers' representatives to the report of the Expert Group should also be taken into consideration.

The report encourages further liberalisation of processing of private credit profiles. The trend in most Member States is to consider such processing a form of 'blacklisting' or profiling. The recurrent references to 'local data protection laws' are not enough, especially as many Member States have not (yet) enacted detailed and balanced provisions on the data protection aspects of credit information. Moreover, the Expert Group's report needs to be improved regarding the provision of precise and specific guarantees on data protection rules.

Chapter Two

Main Developments in Member States



Austria

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

The project described in the 2008 Report Year, regarding the modification of the Austrian Data Protection Law, was taken up afresh and agreed upon by parliament at the end of 2009 with the title **Datenschutzgesetz Novelle 2010** (*Data Protection Law Novella 2010*)[7]. In this new draft legislation[8] only some of the issues dealt with in the 2008 draft legislation were adopted. The main innovations adopted concern regulations with regard to video surveillance, the introduction of a data breach notification obligation in serious cases and simplification of the notification of the use of data by changing to an online notification process. The proposal in the original draft legislation to create a legal basis for the obligatory appointment of a data protection officer was abandoned.

The Austrian Data Protection Commission will report on the details of the amendment and its effects next year, since the amendment only came into effect on 1.1.2010.

A new draft legislation for the implementation of Directive 2006/24/EC (**data retention**) was sent for approval at the end of 2009[9]. The Austrian Data Protection Commission has submitted a comprehensive opinion on this draft and indicated[10] again that, in case of such a major interference into the basic right to data protection, the purpose of the use of data must be clearly and conclusively defined, entailing a clear limitation of the concept of "serious criminal offence".

During the reporting period numerous complaints were submitted relating to **credit information**. Therefore, the Data Protection Committee repeatedly expressed its earlier demands for a definition of the regulatory framework for the identification, the offer and the further use of credit ratings at several occasions. As a result the responsible federal government department was instructed to present draft legislation by the end of 2010.

The Data Protection Commission expressed the need for urgent legislative actions in another sector, namely that of the exchange of data between health care providers (e.g., hospitals) and private health insurance companies. The DPC conducted an in-depth analysis together with the representatives of the concerned interest groups (insured persons, insurers, hospitals, medical profession) and made it available to the federal government department responsible for drawing up the draft legislation.

B. Major case law

The existence of a right to **information** regarding data recorded in the course of **video surveillance** was refused in a case in which

- the regular storage time was 48 hours,
- no event calling for analysis had occurred and
- other persons would have most certainly also been affected by the filming and thus also by the analysis.

This decision was based on the fact that data protection rights of third parties – that is, the other persons filmed - in the said situation have priority over the applicant seeking information, as the data will have been deleted in any case already after a very short time, and will until then not have been made available to anyone, as there was no cause for analysis (such as vandalism, assault on persons, etc.)[11].

As has also been confirmed meanwhile by the constitutional court, **storage of (criminal) procedure documents** is admissible beyond the duration of the procedure, even in cases where the suspect has been acquitted or the procedure has been abandoned. This holds good despite the fact that, alongside the basic principle that data may be kept only for as long as necessary, there is no specific legal provision on the permissible storage period of procedural documents in force. The essential reason for storing procedural documents after the end of the procedure is the need for demonstrating an acquittal or the abandonment of

[7] http://www.parlament.gv.at/PG/DE/XXIV/I/I_00472/pmh.shtml

[8] The draft and all comments can be downloaded from the following website of the Austrian Parliament: http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00062/pmh.shtml

[9] http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml

[10] http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117_I3/imfname_178831.pdf

[11] http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20081205_K121385_0007-DSK_2008_00/DSKTE_20081205_K121385_0007-DSK_2008_00.pdf

a procedure, as well as the possible need to check the legitimacy of the way the procedure was conducted. The danger of general abuse of data through further use for a new purpose that is different from the original purpose for which it was communicated is not to be countered by the prior erasure of the procedural documentation, but rather by means of precisely defined limitation of access that is also efficient from a technical and organisational point of view[12].

C. Major specific issues

E-voting. From 18 May to 22 May 2009, those studying in Austria could vote for their representation of interests electronically, using their citizen's card[13]. In the voting system, the voters' respective identity data and the content of the respective votes cast were encrypted separately from each other. When counting the votes, the identity data of the voters were decrypted with the service provider's secret key. Thereby all the votes cast by non-authorised persons were removed from the electronic urn. The identity data were at once removed from the database and erased. The content data (votes), which were still encrypted with the election committee's key, were then mixed and, with the help of the secret private key of 2 members of the election committee, unlocked and counted. During the entire electronic voting procedure, no names were used as identity data, but exclusively specific personal identification indicators attributed by the Data Protection Commission for the index of voters. In order to check the right to vote, these were compared with the specific personal identifications of the students who had used the citizen's card during the voting procedure.

[12] http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20090121_K121390_0001-DSK_2009_00/DSKTE_20090121_K121390_0001-DSK_2009_00.pdf

[13] http://www.oeh-wahl.gv.at

Belgium

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

Flemish Supervisory Committee of Electronic Administrative Data Flows

The Flemish Supervisory Committee of Electronic Administrative Data Flows (*Vlaamse toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer* – hereafter "Supervisory Committee" or "FSC") authorises the exchange of personal data through electronic data flows between all departments of the Flemish administration, the provinces, cities and municipalities. Moreover, upon request or of its own accord, it advises the Flemish Parliament, the Flemish government and other authorities and stakeholders. In some cases, a security officer can only be appointed after a positive opinion of the Supervisory Committee. The FSC reports to the Flemish Parliament every year. In its meeting of 17 December 2009, the members of the FSC were appointed by the Flemish Parliament. The FSC was established with the Flemish Decree of 18 July 2008 *on electronic administrative data flows* (the so-called "e-gov decree"). The FSC's chairman and two of its members were appointed by the Commission for the Protection of Privacy (hereafter "the Commission" or "the Belgian Commission"), and three other members were appointed by the Flemish Parliament, assisted by an advisory expert selection committee.

Developments regarding the legislation on camera surveillance (Opinion Nos. 24/2009 and 40/2008)

Since the Act *regulating the installation and use of surveillance cameras* (hereafter "the Camera Act") entered into force on 10 June 2007, the Commission has received over 6,000 notifications. An important principle of the Act is that it is not every camera that must be notified, but rather every site under surveillance. Due to a number of practical problems experienced by the police services when using mobile surveillance cameras, in 2009 the Commission received an invitation from the Senate Committee for Internal Affairs to participate in the evaluation of the Camera Act. This parliamentary activity resulted in *the amendment of the Act of 21 March 2007 regulating the installation and use of surveillance cameras* (Belgian Official Journal of 18 December 2009). Thanks to the amended act, it is now sufficient to ask the municipal council in question for an opinion, which, in turn, has to consult the head of the local police, whereas before it was also necessary to ask for the latter's opinion. The amended version of the Camera Act also contains a new chapter stating that mobile camera surveillance can only be used by the police services in the context of large gatherings and exclusively for non-permanent tasks that are limited in time. Camera's may be used both in open places (e.g. during a demonstration) and closed places that are accessible to the public (e.g. a rock festival).

The Royal Decree of 21 August 2009 *amending the Royal Decree of 10 February 2008 establishing the manner of indicating camera surveillance* (Belgian Official Journal of 25 September 2009) also modified the existing rules regarding the dimensions of the compulsory pictogram indicating camera surveillance.

B. Case Law

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

C. Major specific issues[14]

Public sector

Central database of vehicle data (Opinion No. 06/2009)

In 2009, the Commission issued a favourable opinion in relation to the Draft Act *on the creation of the central vehicle database*. This database's main purpose is to track vehicle owners (through their registered owners). Two of the Commission's previous annual reports show that it issued a negative opinion on two earlier drafts (Opinions 42/2006 and 23/2008). The new draft takes into account almost all of the Commission's observations and contains substantial improvements, including the clear appointment of a controller and the addition of a clear list of purposes for which the data from the central database may be used. A list of possible (categories of) recipients of the data is described in general terms and the power of authorisation of the Sector Committee of the Federal Authorities (established within the Commission and partially composed of Commission members) has

[14] All of the Commission's opinions, recommendations, authorisations are available on its official website: http://www.privacycommission.be.

been recognised. Moreover, this Committee has been entrusted with a large number of advisory competences. The Commission also pointed out a few possibilities for improvement, however. The draft would have to explicitly mention, for example, that number plate data (from the current register of vehicles) will be included in the central database. It is recommended to give a better description of how the managing institution for the sector[15] and all data sources (e.g. car inspection centres and manufacturers) would have to comply with the duty to inform the data subjects, and of the concrete measures to be taken in order to effectively appoint the person in charge of information security. The Commission also advises that any service or data source having access to the data should inform the data subject, the managing body and the Sector Committee of security breaches. This so-called "security breach notification" is new for Belgium, but does exist in English-speaking countries and will also be included (partially) in the planned modification of "E-Commerce Directive" 2002/58/EC.

General authorisation of access to the register of number plate data (Deliberation FA No. 12/2009)

In the past it was very unclear for private administrators of public parking facilities how they could collect parking fees, as reflected in several sentences issued in this context. That is why the Belgian Commission and the Sector Committee of the Federal Authorities (supervising the electronic disclosure of personal data within the Federal Authorities) always refused to grant private parking administrators access to the identity of number plate owners in the DIV[16] database (Opinion No. 37/2003 and Deliberation FA No. 02/2007). Thanks to an amendment (Act of 22 December 2008 *on various provisions*, title 4, chapter 2, Belgian Official Journal of 29 December 2008) the situation has been clarified, and cities and municipalities, their parking administrators and autonomous municipal enterprises have been authorised to ask the DIV for a number plate owner's identity. This is a so-called "general" authorisation, meaning that, in the authorisation, the Sector Committee describes the (strict) conditions the DIV and the categories of beneficiaries must meet, and that the beneficiaries must sign a model agreement committing them to meet these conditions.

In order to increase transparency, all general authorisations of the Commission's Sector Committees and the lists of beneficiaries are published (in French and Dutch) on the Commission's website in the "Decisions" section.

The processing of personal data in the context of doping-free sports (Opinion No. 30/2009)

At the request of the relevant minister, in 2009, the Commission issued an opinion on the "International Standard for the Protection of Privacy and Personal Information", elaborated by the WADA (World Anti-Doping Agency). This International Standard contains a minimum of common rules that must be observed when processing personal data on the basis of the World Anti-Doping Code. The Commission has observed that the International Standard does not always respect the safeguards which must be offered under the Belgian privacy regulations and made a few remarks, for example, about the possible grounds for processing sensitive personal data, the duty to inform the data subjects, security measures and liability, the retention period of personal data and the exercise of the data subject's rights (right to access, objection and rectification). The Commission also pointed out that the minimum standards described in the International Standard cannot prejudice the stricter Belgian privacy regulations.

Following a request for information, the Commission also issued an opinion about the Flemish regulations regarding the fight against doping in sports, more particularly the obligation to disclose the so-called "whereabouts" information with a view to out-of-competition doping controls. The Flemish Decree of 13 July 2007 *on medically and ethically acceptable sports* and the Decree of the Flemish Government of 28 June 2008 implementing the former decree do not establish which whereabouts information top-level athletes must communicate. They do, however, refer to the World Anti-Doping Code, a reference which is currently under appeal before the Council of State. The Commission nevertheless held that requesting whereabouts information for four hours a day is proportionate. The Commission made some observation related to the status of elite athletes. Finally, the Commission made a number of remarks

[15] The Directorate-General for Mobility and Road Safety of the Belgian Federal Public Service for Mobility and Transport.

[16] *Directie Inschrijving Voertuigen* – the Belgian federal office in charge of registering vehicles and their drivers.

about maximum data retention periods and the duty to inform the data subject.

Database for the Walloon public service for professional training and employment (Opinion No. 18/2009)
In 2009, the Commission issued a favourable opinion on the "Jobpass" system of the "*Service public de l'emploi et de la formation professionnelle*" (the public service for professional training and employment - hereafter "Forem"). Forem is a Wallonian organisation acting in the public interest carrying out tasks in partnerships pursuant to the administrative agreement between the Walloon government and the Forem's Board of Directors. On the one hand, the Jobpass system provides the unemployed with a chip card, and on the other it implements a new database. The objective of the database and the chip card is to make it easier for the Forem and its partners (e.g. training centres, which only have access to the information necessary to perform their tasks) to identify the unemployed and exchange information about them. The system also facilitates the exchange of certain information with the Federal Employment Service (through the Crossroads Bank of Social Security) and helps the unemployed to compile proof of their efforts to find a job: with their chip card, they can register visits to the Forem's organisations and partners without having to see an employment consultant. The Commission was of the opinion that these data processing operations were adequate, relevant and not excessive. It did, however, prohibit the use of the National Register number (which was on the secured part of the chip card), since this had not been authorised by the Sector Committee of the National Register.

Private Sector
Direct Marketing (Recommendation No. 04/2009)
After consultation of all European DPAs and on the basis of several requests and complaints received in the past few years, in 2008, the Commission published a legal memorandum expressing its position on direct marketing practices. To come to a balanced analysis, the Commission then started a dialogue with stakeholders from the world of business, consumer association and academic sectors in order to learn more about their interests, priorities and codes of conduct, if any. Finally, the Commission wanted to hear the citizens' opinions and, therefore, posted a public survey on its website. These efforts resulted in Recommendation No. 04/2009 on direct marketing and the protection of personal data. In this document, the Commission gives its interpretation of the Privacy Act with regard to direct marketing, it recommends a number of ways of working that can be considered as best practice (which favour fair and transparent data processing operations, regardless of whether this is established by law) and it makes a few recommendations to the legislator in order to improve the existing provisions.

Consent
The Commission is of the opinion that the free, informed and specific consent of the data subject can serve as a basis for the justification of direct marketing and also recommends this as best practice. The recommendation specifies conditions and points out a number of cases in which consent is strictly required (e.g. almost always when direct marketing is practised using text messages, e-mail, fax or automated dialling systems) or as good as inevitable (e.g. list brokering and profiling).

Legitimate interest
Although maintaining a balance is far from obvious (especially for list brokering and profiling), the Commission acknowledges that this principle is a basis for the processing of personal data in the case of direct marketing. The recommendation stipulates the moment to assess the balance of interests, the criteria and ways to do so. If this balance is disturbed, the processing must be stopped at once.

Retention period
On top of the duty to rectify incorrect data, the Commission also recommends a personal data retention period.

Information
The Commission underlines the importance of correct information, especially when the data was not obtained directly from the data subject. In this case, the Commission highly recommends that the controller proactively disclose the data source. Direct marketers cannot invoke an exemption from the duty to inform the data subject due to impossibility or disproportionate effort, partially because contacting the data subject is at the heart of direct marketing.

Objection
Finally, the Commission mentions the data subject's free right to object without giving any reason. This objection is sufficient to terminate the processing operation. It also states that no conditions must be linked to this right.

Recommendation to landlords and property estate agents about the processing of personal data of candidate tenants (Recommendation No. 01/2009)
In the last few years, the Commission's secretariat regularly received questions from citizens about lease agreements and the personal data that owners of rented homes and property estate agents can request. In its recommendation, the Commission stipulates which data can and cannot be requested.

The Commission considers that data such as one's surname, first name, address, legal entitlement to stay in Belgium and the date of birth are necessary to enter into a lease agreement, but that it is disproportionate to ask for the ethnic origin, the place of birth and the National Register number of candidate tenants. Their marital status, phone number and number plate may or may not be relevant. It is prohibited, for example, to process tenants' number plates, except when the rented home has a parking spot requiring vehicle recognition, for example to grant the tenants access or to supervise the parking spot. Conversely, the marital status is not relevant for a tenant that will be the sole occupant of the rented home.

Landlords must be able to check whether tenants are solvent enough to pay the monthly rent, for which it is sufficient to know their regular income. Asking for the candidate tenants' global financial situation is not necessary. This means that it is justified for the latter to have to show their payslip (having crossed out their employer's identity, profession and other irrelevant data if they prefer), but they do not have to give the landlord a copy of the slip, since it is sufficient to see that the candidate tenants are solvent. It is acceptable, however, that property estate agents keep proof of this check of candidate tenants' income by making a copy of the slip. Data from the Belgian Central Database of Credits to Private Persons are reserved for credit grantors and organisations or individuals with a similar function, for the performance of their duties.

Landlords can request data about the persons that will occupy the rented home, for example, how many of them there will be and their approximate age. Excerpts from the criminal record are prohibited under the Privacy Act. The processing of data relating to candidate tenants' health is only authorised, according to the Commission, if two conditions are met. First of all, the tenant must give his written consent, which can be revoked at any time. Secondly, the data must be relevant: a disabled person interested in an apartment adapted to his needs may, for example, have to describe his state of health.

New Technologies
Data Retention (Opinion No. 20/2009)
In the context of the transposition of European Directive 2006/24/EC, the so-called Data Retention Directive, into national law, the Commission was asked to issue an opinion about a draft act and a draft royal decree regarding the duty to cooperate. The Directive aims to harmonise the obligations of service providers with respect to retaining certain data and making them available to authorised services in the context of investigating, tracking and prosecuting serious crime. The Commission has already twice issued a negative opinion in this context. In 2009, however, a positive opinion was issued on the adapted drafts. Nevertheless, a few remarks should be taken into account. The data retention period, for example, must be reduced from 24 to 12 months and must be established in the draft act. Parliament must assess the draft act and the draft decree and the relevant competent minister must report to Parliament every year. Finally, the role of the NTSU-CTIF service[17], having direct access to the databases, needs to be defined more clearly. More concretely, its place in the organisation chart and the appropriate level of security must be clarified.

Radio Frequency Identification (Opinion No. 27/2009)
In this opinion, issued by its own initiative, the Commission stipulates the conditions for processing personal data by means of radio frequency identification (RFID) tags. With this technology, information stored on chips implanted in objects or living beings can be stored and read remotely. The Commission points out two situations involving a processing operation of personal data, on the one hand linking personal data with a tag,

[17] The central technical interception service of the federal and local police services.

and on the other hand placing personal data on a tag. In the opinion, the Commission lists the principles of the Privacy Act the controller has to take into account. The processing operation must be legitimate and proportionate, for example. The data subjects' consent can be a basis for a processing operation, but the weight of the controller's interest also needs to be assessed in comparison with the data subject's right to protection of his privacy, for example, through risk analysis. The data subject also needs to be informed sufficiently through a privacy policy that is easy to understand, containing at least the controller's identity and address, the purpose of the processing operation, the data that will be processed (possibly including tag monitoring), a summary of the privacy assessment and a risk analysis. Finally, the Commission emphasises the importance of adequate technical and organisational security measures.

Bulgaria

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

1. At its first meeting in 2009, the Commission for Personal Data Protection adopted new Rules on the Activity of the Commission for Personal Data Protection. It was promulgated in the State Gazette of 2 February 2009, repealing the Rules on the Activity of the Commission that had been in force since March 2007.

   The need to prepare and adopt the 2009 Rules was based on the new priorities adopted by the Commission for Personal Data Protection in its capacity as an independent supervisory authority in the field of personal data processing. This legal act aims to synchronise the activity of the administrative units of the Commission by exercising overall control on observance of the personal data protection law and personal data processing. The regulations set out in the Rules gave the Commission greater flexibility when adopting decisions, thus raising the efficiency of the Commission's activity as a whole.

   These Rules emphasise the powers of the Commission specified in the Personal Data Protection Act and the related proceedings carried out by the Commission. Structural changes in the administration of the Commission were made, consolidating the units assisting the Commission in a particular activity. In this way, expert activity was consolidated, which led to better results through the implementation of the Commission's powers defined in the legislation.

2. The CPDP prepared a draft amendment and supplement of the Personal Data Protection Act (PDPA) and in February 2009 it organised and held public discussions with the participation of the Chairperson and members of the Internal Security and Public Order Committee at the National Assembly, representatives of non-governmental organisations, academic circles and the media. Due to the parliamentary elections in June 2009, the draft law was not approved by the 40th National Assembly. The work on it continued and the recommendations from public consultation were taken into account.

3. Representatives of the CPDP took part in the work of the intra-departmental working party for the preparation of a draft Law Amending and Supplementing the Electronic Communication Act. The envisaged amendments stipulate that the Commission for Personal Data Protection will be the monitoring authority in order to exercise control over the activity of the enterprises providing public electronic communication networks and/or services, ensuring the observance of the rules on protection and security of the stored data pursuant to the provisions of Art. 7 of Directive 2006/24/EC. The establishment of the Commission as the monitoring authority is in accordance with the obligation of each Member State under Art. 9 of Directive 2006/24/EC to determine a public authority responsible for the monitoring, in its territory, of the implementation of the regulations adopted by the Member States in accordance with Art. 7 on stored data security. Directive 2006/24/EC explicitly stipulates that this authority may be the body established under Art. 28 of Directive 95/46/EC, and in the Republic of Bulgaria this authority is the Commission for Personal Data Protection.

4. In November 2009, the Council of Ministers approved the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data concerning supervisory authorities and transborder data flows, and made a proposal to the Parliament to ratify it. The Parliament subsequently ratified it and the Protocol was promulgated in the State Gazette of 6 January 2010. The CPDP is the supervisory authority under Art. 1, para.1 of the Additional Protocol.

B. Major case Law

The handling of individuals' complaints about specific violations of their rights is a significant part of the Commission's activities. The analysis shows that the complaints filed against the central law enforcement authorities mainly concern the provision of personal data

to third parties or personal data dissemination without the individuals' knowledge and consent.

A substantial number of complaints also concern the refusal of access to personal data, as well as provision of personal data to third parties. The Commission for Personal Data Protection issued compulsory instructions for providing access to personal data in accordance with the requests of the claimants, which were considered well-grounded.

In 2009, the Commission for Personal Data Protection was approached with new cases concerning the dissemination of personal data on the Internet. It was established that personal data from a particular category of users is distributed in forums as part of scholarly papers, reports, lectures, and analyses for the purpose of providing support. Aside from the violations of the Copyright Act and Related Rights, the Commission for Personal Data Protection considers that the distribution of personal data contradicts the principle of proportionality and purpose limitation of the processed personal data under Art. 2, para. 2, p. 2 and p.3 of the Personal Data Protection Act.

In 2009, the Commission expressed opinions in response to requests submitted both by data controllers pursuant to Art. 3 of LPDP and by individuals with respect to their legal rights. Answers have been provided to the enquiries concerning the publication of the personal data of owners, representatives and members of collective bodies of commercial companies in the Trade Register, maintained by the Registry Agency. According to Art.11 of the Trade Register Act, the Register is public. Everyone is entitled to have free access to it and to the electronic image of the documents based on which entries, erasures and announcements were made, as well as the electronic image of the company cases of the re-registered entrepreneurs. The Agency also provides free access to applications contained in the information system of the Trade Register, the attached documents and the declared refusals. The company's details, such as registered address, management address and company representatives become public data after the registration of the company in the Register. Ordinance No. 1 on Trade Register maintenance, storage and access specifies the standard forms of the registration applications and explicitly indicates the circumstances requiring registration and which should be entered on the applications for registration, erasure or publishing. The Ordinance regulates the statutory obligations on the grounds of which the Registry Agency lawfully processes the personal data of a particular category of individuals.

Enquiries have been submitted concerning cases in which employees in various retail outlets, when executing payments with debit and credit cards, referred to as Electronic Payment Instruments (EPI), ask individuals to present their identity document - ID Card - in order to check their identity. In accordance with Art. 31, para. 5 of the Money Transfer, Electronic Payment Instruments and Payment Systems Act, the trader may request the identity document if there are reasonable doubts concerning the identity of the EPI holder.

With regard to the implementation of Art. 64 of the Judiciary System Act concerning the provision of publicity and transparency of court operations and publicity of court rulings and in connection with the protection of individuals rights in relation to personal data processing, the Commission has expressed an opinion that, by establishing and maintaining a public register of court rulings, certain measures should be taken in order to prevent individuals from being identified. Besides the use of initials instead of individuals' names and the removal of personal numbers and addresses, all indications related to physical, physiological, genetic, mental, psychological, economic, cultural, and social details or any other factors helping to identify the individual despite the use of initials, should also be removed.

C. Major specific issues

On 30 April 2009, at an extraordinary meeting, the Commission for Personal Data Protection entered in the Register of personal data controllers and the registers kept by them all unregistered data controllers who had filed an application within the period from 2003 to 2008. 193,351 personal data controllers have been given identification numbers. With this decision, the Commission determined a deadline for data controllers to update the submitted data for the purpose of ensuring that the database is current. The obligation to update the circumstances in the registries is a constant

obligation under the Personal Data Protection Act. The Act provides for sanctions for unregistered personal data processing and incomplete update of their details on the registration form, that should be entered in the register. The decision of the Commission to update the information up to 15 February 2010 was made with the purpose of guaranteeing the reliability of the information in the public register which is generally accessible on the Internet site of the institution. The data controllers are given the opportunity to update their information on the Internet - even without electronic signature - by post and in person with the Commission reception.

Cyprus

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

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

(II) Laws amended

(III) Laws enacted

B. Major case law

Pursuant to a question submitted by the Chief of Police to the Law Office of the Republic regarding the lawfulness of a Statutory Regulation providing for the collection of third countries' students' fingerprints upon their arrival in Cyprus, the Attorney General issued an Opinion concluding that this practice does not seem to be lawful and suggested that the Commissioner for Personal Data Protection should further consider the subject.

Having examined all the relevant legislative regulations in place, the Commissioner issued a Decision concluding that this specific Regulation does not constitute/provide a legal basis for the collection of the aforementioned fingerprints. Subsequently, a procedure for imposing administrative sanctions to the Police was initiated but not concluded since in the meantime, the Chief of the Police had proceeded to destroy the fingerprint database in line with the above Opinion and Decision and of his own accord.

Pursuant to publications in the daily press and a number of phone calls to our Office by concerned citizens regarding a practice by Municipal Authority Traffic Wardens of photographing illegally parked cars whose owners had been given penalties, our Office, in correspondence with the Municipal Authority, expressed the view that this practice was in breach of data protection legislation.

Although the Municipal Authority terminated this practice in compliance with the above view, it then submitted a challenge before the Supreme Court. The case is pending.

C. Major specific issues

Pursuant to a proposal submitted by the Commissioner, in October 2009, the Council of Ministers adopted a Decision according to which all Ministries and Government Departments/Services should appoint Data Protection Officers, who would subsequently be trained by the Commissioner's Office to deal with internal data protection issues.

Following a number of complaints submitted to our Office, in 2003, the Commissioner issued an Opinion concluding that the National Guard's practice of including the medical (physical or mental) reasons for which soldiers were dismissed or temporarily suspended from service obligations on soldiers' Temporary Service Dismissal/Suspension Documents was in breach of the data protection legislation.

The National Guard terminated this practice in compliance with the above Opinion. In 2009, however, the Minister of Defence issued a Decree directing the National Guard to reinstate the terminated practice, on the grounds that the issuance of Temporary Service Dismissal/Suspension Documents is an Administrative Act, which obliges the Administrative Body, i.e. the National Guard, to communicate in writing to the soldiers, the reasons for which the Decision outlining the dismissal/suspension was based. The case is before the Commissioner and a decision is pending.

The Association of Cyprus Banks (ACB) informed the Commissioner of its intention to develop and establish the "ARTEMIS" system/database, which would be operated by a private organisation reporting to the ACB, in order to enable the ACB's member banks to share information on bad debtors and to assess potential clients' credit status.

The ACB submitted the organisation's draft internal Rules to our Office for the establishment and operation of this system/database, which was finalised and adopted in compliance with the Commissioner's comments/recommendations. The Rules were brought into effect and the system has been operational since November 2009.

A private company that intends to launch a service similar to *Google Street View* asked for our Office's views

on the subject. The proposed service involves taking photographs of all the public streets in Cyprus and creating a virtual map which will be available on the web for visitors to take virtual tours. Potential applications include the service being used by Municipal Authorities for identifying locations that require road works.

Taking into account the relevant documents adopted by Art. 29 WP, our Office informed the company that, alongside other safeguards, the photographs should be blurred in a way that would prevent exposing vehicle number plates and people's faces. Furthermore, the service should provide data subjects with an easy way to submit complaints regarding exposed personal data. Our Office is currently scrutinising the proposed service.

Czech Republic

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

The basic legal regulation in the area of personal data protection is Act No. 101/2000 Coll., on the protection of personal data and amendments to some related acts, which entered into effect on 1 June 2000. The Office for Personal Data Protection ("OPDP" or "the Office") was established on the basis of the provisions of this Act and has strong powers at its disposal, including taking measures and direct imposition of fines in case of breach of law, as well as being an independent body. The Act essentially implemented Directive 95/46/EC into the Czech legal order. With effect from 26 July 2004, Act No. 101/2000 Coll. was amended by Act No. 439/2004 Coll., and was thus made fully compliant with the aforementioned Directive.

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

In 2008, a procedure to amend the Electronic Communications Act No. 127 resulting from the need to transpose Data Retention Directive No. 2006/24/EC into national law was completed.

Since 1 April 2009, when Act No. 52/2009 Coll. added definitions of new offences to the Personal Data Protection Act, the Office has been obliged to prosecute conduct consisting of a breach of the prohibition of publishing personal data stipulated by other legal regulations. This amendment accompanied the "Muzzle Act", a change in the Code of Criminal Procedure which responded to repeated publication of large quantities of personal data coming from criminal proceedings, mostly in tabloids, and also in relation to minors. The Office considered it positive that the amendment particularly pointed out the dangers associated with unrestricted publication and bulk disclosure of personal data (including publication in the media and on the Internet). Unfortunately, within the public debate accompanying this change in the criminal procedure, or rather a critical campaign in most media concentrating on the alleged suppression of the freedom of speech, the original objective of the amendment was often neglected: to protect the privacy of persons injured in crimes (the victims).

Act No. 111/2009 Coll. on basic registers imposed a duty on the Office, within the newly created eGovernment system, to establish "source" and "agenda" identifiers of natural persons and to provide for transfer of the agenda identifiers of natural persons within the individual electronic agendas. The new identifiers should, among other things, reduce the risk of unauthorised processing of citizens´ personal data stored in state registries. The Office accepted the mentioned competence on the condition that the creation and transfer of identifiers would take place in a way that would ensure maximum security and on the condition that the entire process of generating the identifiers would be strictly separated from any actual processing of personal data by the authorities. At the same time, the current supervision by the Office of personal data processing within the existing state registers and the newly proposed basic registers is in no way prejudiced.

B. Major case law

In 2009, the Office's legislative activities were concerned with specific laws having impacts on privacy and data protection (during the Government lawmaking procedure it is obligatory for the Office to be consulted). Attention was particularly focused on the preparation of the new codification of civil law, the work on new electronic registers of public administration and regulations related to healthcare registers. The Office's comments and objections were partly taken into consideration.

C. Major specific issues

When enforcing national law, and by extension EU/EC law, ***control and verification work***, including on-the-spot inspections, continues to play a key role. In conformity with Article 31 of the Personal Data Protection Act, the Office's control

activities are pursued either based on a control plan or on complaints. The control plan is drawn up jointly by the President and inspectors of the Office – the document is binding and its fulfilment is regularly evaluated at a meeting of the board of inspectors, which serves as a joint advisory panel for the President and inspectors. Most of the controls including on-the-spot inspections related to breaches of the DP Act were carried out on the basis of complaints and instigations (90%). The remaining control activities derived from the Control Plan (8%) and the instructions of the President of the Office (2%). It should, nevertheless, be noted that the last two categories of inspections mainly involve more complex control procedures.

Special attention when establishing the 2009 Control Plan was paid to the following areas:
Public administration information systems - processing of personal data was a frequent subject of inquiries and requests for consultation (controls were concerned with record of the population).
Multinational information systems - the controls were mostly initiated by the joint supervisory bodies SIS and EURODAC and other EU initiatives (i.e. traffic data in transport systems).
Personal data processing in the use of camera surveillance systems - the Czech DPA has applied the basic personal data protection principles published in the official DPA position.
Information systems on the area of justice - the Czech DPA encountered personal data processing in relation to activities including administrative sanctions.

In cases where the control indicated violation of the DP Act, administrative proceedings were pursued against the relevant parties for offences related to the (illegal?) processing of personal data. In those cases, fines were imposed. Those liable to the proceedings can lodge an appeal against the decision with the President of the Office.

Statistical data on complaints addressed in 2009:

Total	879
of which:	
submitted for control	129
submitted for commencement of proceedings	43
forwarded to other competent bodies	24
suspended with notification	683

The above-mentioned control activities do not include those concerned with ***unsolicited commercial communications*** ("marketing spam"). In 2009, this special agenda involved 2261 instigations/complaints, of which 1678 instigations/complaints were resolved; 131 controls were completed and 112 sanctions were imposed.

In the high priority framework of ***public relations and awareness***, in 2009 the Office continued to develop the tradition of organising balancing press conferences; however, communication with the media was focused mainly on everyday service and provision of topical information on the website.

The yearly competition for children and teenagers "This is my private space! Don't look and don't poke about!" was also launched in 2009 and the Office noted greater participation and a shift in quality. The awards for the winners were traditionally presented as part of the Zlín International Festival of Films for Children and Teenagers. The children's competition entries were exhibited at the beginning of the new school year in the anteroom of the Senate Meeting Hall and on several other occasions.

2009 marked the third year of the Office's ongoing teacher training programme concerned with personal data protection in education within a three-year accreditation by the Ministry of Education, Youth and Sports. Approximately 200 teachers participated in a workshop in which the Office provided the relevant expertise.

The Office also considered it important to meet with senior citizens (in cooperation with the Third Faculty of Medicine of Charles University), for whom it is necessary to regularly explain the meaning of personal data protection, and raise their awareness of the fact that they have a right to protection of privacy.

A workshop concerning the issue of DNA profiles, which was initiated on the basis of the Office's control findings, was organised in the Senate under the auspices of its Vice-President in the autumn of 2009. The workshop raised a number of issues that require a precise legislative basis.

Denmark

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

The Act on Processing of Personal Data (Act No 429 of 31 May 2000) was adopted on 31 May 2000 and came into force on 1 July 2000. The English version of the Act can be found at the following address: http://www.datatilsynet.dk/english/the-act-onprocessing-of-personal-data/

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

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

- The Danish Constitution;
- Act on Marketing Practices, Section 6 (cf. Act No 1389 of 21 December 2005);
- Act No 429 of 31 May 2000 on Processing of Personal Data;
- Act on Competitive Conditions and Consumer Interests in the Telecommunications Market (cf. Exec. Order No 780 of 28 June 2007);
- Executive Order No 714 of 26 June 2008 on the Provision of Electronic Communications Network and Services;
- Chap. 71 of Law on Administration of Justice, cf. Exec. Order No 1069 of 6 November 2008;
- Section 263 of the Penal Code, cf. Exec. Order No 1068 of 6 November 2008.
  According to Section 57 of the Act on Processing of Personal Data, the opinion of the Danish Data Protection Agency (DPA) shall be obtained when orders, circulars or similar general regulations of importance for the protection of privacy in connection with the processing of data are to be drawn up. The provision also concerns bills. In 2008 the DPA gave its opinion on several laws and regulations affecting privacy and data protection.

In 2009 there were two amendments to the Danish Act on Processing of Personal Data:

- A new section 72 a of the Danish Act on Processing of Personal Data was adopted to implement Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
- A new subsection 3 to section 1 of the Danish Act on Processing of Personal Data was adopted. Until 2009, the Danish Public Administration Act applied to manual exchange of personal data between public bodies. As a consequence of this amendment, the Danish Act on Processing of Personal Data now applies to manual disclosure of data between public bodies.

B. Major case law

The DPA has handled several cases regarding online social networks.

The online social networks collect large amounts of the users' personal data and possess large amounts of information.

Social networks are a developing area and new challenges regarding protection of personal data constantly arise along with the technological developments and the new privacy settings on the social networks' websites.

In Denmark, Facebook has received a lot of press coverage, and many citizens have contacted the DPA regarding Facebook. According to Facebook, there are more than two millions Danish users of Facebook.

The DPA started a dialogue with Facebook in April 2009 and raised a number of questions – partly based on enquiries from Danish users – regarding Facebook's processing of personal data.

Furthermore, the DPA has asked Facebook for more information on any data sharing with third parties that takes place with the different applications.

The DPA is still in dialogue with Facebook. More information and advice about social networks, as well as the letters from Facebook, can be found on the DPA's website, www.datatilsynet.dk

C. Major specific issues

Video Surveillance in general
In 2008 and 2009, the DPA handled several cases regarding video surveillance. Some of these cases were complaints over unjustified disclosure of data. Others were cases initiated by the DPA on its own initiative, due to press coverage, for example. Most of these cases deal with illegal disclosure of video surveillance data containing personal data via the internet or to the press.

In 2008 and 2009, the DPA reported some of the cases regarding violation of the rules of chapter 6a on video surveillance in the Danish Act on Processing of Personal Data to the police.

A few of these cases have come to trial, and in these cases some claims have been dismissed due to the courts view of the merits of each individual case. In other cases, where the DPA has reported violations, the companies in charge have accepted a fixed penalty notice.

In 2009, the DPA did not find cause for police reporting as many cases of violation of chapter 6a of the Danish Act on Processing of Personal Data as in previous years. The DPA estimates that this is due to the press coverage of some of the earlier cases which were reported to the police.

Video Surveillance in taxis
In 2009, the Danish Road Safety and Transport Agency consulted the DPA regarding a Danish Parliamentary draft decision on video surveillance in taxis. The DPA's comments on the draft were critical regarding a number of issues.

Later in 2009, the DPA commented on a bill that made it mandatory to have video surveillance in taxis. This bill was based on the Parliamentary draft decision regarding video surveillance in taxis, which the DPA earlier had given critical remarks, and the DPA also made a number of comments on the bill.

The bill introduces an obligation to install video surveillance in taxis with regard to help solving cases of robberies and violent attacks on taxi drivers. Furthermore, the bill will help prevent and solve robberies and violent attacks on passengers.

The bill is expected to be tabled in spring 2010.

Estonia

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

Directive 95/46/EC is implemented in the Estonian Personal Data Protection Act (the English version is available on the Inspectorate's website: http://www.aki.ee/eng/?part=html&id=105). The new version of the Act started to apply from 1 January 2008. Since then, there has been no modification to the legislation on personal data protection.

The Directives 2002/58/EC and 2006/24/EC are implemented in the Electronic Communication Act (the latest translation is not yet available). The obligation to collect and retain traffic data was enacted in 2007. The data retention that concerns the fixed network telephony data and mobile telephony data came into force as of 1 January 2008. The retention of data concerning Internet access, Internet e-mails and Internet telephony came into the force on 15 March 2009. Therefore, since 2009, all Estonian telecommunication service providers have been obliged to collect traffic data, as has also become evident during the supervision proceedings conducted by the Inspectorate.

B. Major case law

With regard to blogs and social networks
The Estonian Data Protection Inspectorate receives many complaints regarding the use of personal data without consent in blogs or social networks. In most cases, requests were made for the removal of pictures or other personal data. At the same time, the Inspectorate had to take into consideration that, in some cases, the reason for the complaint related to disagreement between two persons, which meant that the data or photos were made public as an act of revenge. Unfortunately, as public awareness continues to increase, these kinds of cases are becoming increasingly common. The Inspectorate takes the position that these kinds of issues should be discussed in the civil courts and not by the data protection authority.

In some cases, the Inspectorate interprets blogs as "public journalism", and thus are subject to the same principles as professional journalism. The disclosure of personal data for journalistic purposes is regulated in the Personal Data Protection Act as follows:

Personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject if this is in the predominant public interest and in accordance with the principles of ethical journalism. Disclosure of information shall not cause excessive damage to the rights of a data subject.

A data subject has the right to demand, at all times, that the person disclosing his or her personal data terminate the disclosure, unless such disclosure is carried out based on law or pursuant to the abovementioned principle and further disclosure does not excessively damage the rights of the data subject. A demand for the termination of disclosure of personal data shall not be made to a person disclosing personal data with regard to data carriers over which the person disclosing the personal data has no control at the time such demand is made.

With regard to online cameras and video-surveillance
During 2009 the Inspectorate carried out supervisory operations relating to online cameras. There have been cases in which public online cameras are configured in such a way that the camera violates the privacy of other people (for example, the camera can be turned and zoomed to view another person's home).

Also, the Inspectorate is carrying out extensive on-site supervisory operations on video-surveillance as a long-term project (for example, in department stores and workplaces). So far the results of the supervisory operations have shown that in some cases even the simple notification is insufficient. According to the Personal Data Protection Act:

Surveillance equipment transmitting or recording personal data may be used for the protection of persons or property only if this does not excessively damage the justified interests of the data subject and the collected data is used exclusively for the purpose for which it is collected. In such case, the consent of the data subject is substituted by sufficiently clear communication of the use of the surveillance equipment and of the name and contact details of the data processor. This requirement does not extend to the use of surveillance

equipment by government agencies derived from and pursuant to the procedure provided by law.

C. Major specific issues

For the third year running, the Inspectorate has chosen priority topics and issued guidelines on these matters. The guidelines for 2009 are only available in Estonian:

- The Processing of Personal Data during Election Campaigns - http://www.aki.ee/download/1101/erakondadekampaaniad_200309%20(2).rtf
- The Processing of Personal Data by the Financial Authorities - http://www.aki.ee/download/1037/AKI%20krediidiasutuste%20juhend.pdf
- The Processing of Personal Data in Genealogical Research - http://www.aki.ee/download/1404/Isikuandmete%20töötlemine%20suguvõsa%20uurimiseks%20171109.rtf
- The Processing of Personal Data in Scientific Research - http://www.aki.ee/download/1469/Isikuandmete%20töötlemine%20teadusuuringus.rtf
- The Use of National ID Codes – http://www.aki.ee/download/1102/Isikukoodi%20kasutamise%20juhis.rtf
- The Personal Data Disclosure of Utility Service Debtors - http://www.aki.ee/download/1240/JUHIS%20%20Korterivõlglaste%20avaldamine%20090309.rtf
- The Right to Request Your Data – http://www.aki.ee/download/1045/kusi_oma_andmeid_090309.rtf

In addition, we have drafted guidelines for holders of public information. The public information guidelines include the maintenance of document registers and data disclosure on the websites of public authorities. The guidelines in Estonian are available here: http://www.aki.ee/est/?part=html&id=125.

Finland

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

The Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999. The Act was revised on 1 December 2000 to incorporate 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.

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

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

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

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

Amendments

During the year under review, there were no actual amendments to the Personal Data Act (523/1999).

The amendment to the Act on the Protection of Privacy in Electronic Communications entered into force on 1 June 2009. The amendment gives association subscribers the right to process identification data in order to prevent and detect illegal use of fee-based information society services, communications networks or communications services or business espionage as referred to in the Criminal Code (Rikoslaki 39/1889).

Illegal use of a communications network or service can be, for example, installation of a device, software or service on the communications network of the association subscriber, opening illegal access to the association subscriber's communications network or service to a third party or other comparable use of the communications network or service if it infringes instructions of use.

The right referred to above does not apply to identification data of fixed or mobile phone network services.

The amendments required by this so-called Lex Nokia were entered in sections 2 and 21 of the Act on the Protection of Privacy in Working Life (Laki yksityisyyden suojasta työelämässä 759/2004) and they entered into force on 1 June 2009.

During the year under review, the amendments required by the directive (2006/24/EC) were entered in the Act on the Protection of Privacy in Electronic Communications (516/2004). The legal obligation to store telecommunications identification data entered into force on 15 March 2009.

In 2006, the Finnish Parliament demanded that the Government begin preparation of legislation on the general protection of personal data in biometric identification. According to the Ministry of Justice, which is responsible for preparing the Act, the general provisions on the processing of biometric identification will be prepared in conjunction with the general review of the Personal Data Act (95/46/EC art. 8 paragraph 7) to be commenced later. However, the Act on Strong Electronic Identification and Electronic Signatures (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009) entered into force on 1 September 2009. It establishes strict quality obligations for providers of identification services. According to the Act, biometric identification can also be used as strong identification.

B. Major case law

The European Court of Justice (Grand Chamber) gave its ruling on the publication of data on earned income on 16 December 2008. The matter related to the scope of application of Directive 95/46/EC, the processing and mobility of personal data on taxation, protection of individuals and freedom of speech. The Court left the definition of the journalistic processing as referred to in Article 9 of Directive 95/46/EC to be established by a national court. However, according to the ruling, the Data Protection Directive must be applied to the processing of personal data derived from public data sources and the use of previously published lists or services**.** The Supreme Administrative Court gave its judgement on 23 September 2009, KHO:2009:82. The Court sent the case back to the Data Protection Board, obligating the Board to send a refusal to Satamedia on their continued publishing of the data. The refusal covered both the publications and the SMS service. The Court stated in its judgement that Article 2.4 of the Finnish Personal Data Act is not in line with the ECJ's interpretation of the scope of application of the directive. The Court reached its decision taking into account the balance between freedom of speech and protection of private life. The Court pointed out that this balance requires that, in relation to freedom of speech, information provided to the audience must have importance in society and not only serve the needs of curiosity. In relation to the purpose of journalism, the Court focused on how these "newspapers" were actually produced. Since the database (register) was printed as such, it could not be created only for a journalistic purpose. The court's decision was that Veropörssi had no legal basis for processing personal data and thus the text message service was also illegal. The Court did not tackle the issues of taxation data as such or the question of the balance between freedom of speech and privacy. The service provider of the SMS service notified the DPA on 28 September 2009 that they would stop the service on 30 September 2009 on the basis of evident illegality. In practice, Finnish newspapers will, in the future, also publish this kind of personal data about persons who are likely to be socially important.

Future amendments to the Finnish Personal Data Act on the inconsistency of Article 2.4. will be prepared by the Ministry of Justice, which recently published a future work plan that also includes an update to the Personal Data Act.

In its decision dated 26 November 2009, the Data Protection Board prohibited Satakunnan Markkinapörssi Oy from processing data pertaining to earned and capital income and assets of natural persons to the extent and in the manner that took place in connection to 2001 tax records. Moreover, the Data Protection Board has prohibited Satakunnan Markkinapörssi from submitting data they have collected and stored pertaining to earned and capital income and assets of natural persons through an SMS service or for any other purpose. The Data Protection Board has also prohibited Satamedia Oy, due to infringement of the Personal Data Act (Henkilötietolaki 523/1999), from collecting, storing and submitting further data pertaining to earned and capital income and assets of taxpayers received from the Satakunnan Markkinapörssi Oy register and published in printed form in a publication entitled Veropörssi. According to information received from the Helsinki Administrative Court, an appeal has been lodged against the decision (communicated on 12 January 2010) of the Data Protection Board. The matter has been transferred to the Turku Administrative Court since the domicile of the company has changed.

The competent Data Protection Board gave its decision on the matter initiated by the Office of the Data Protection Ombudsman on the authentication of quick loan applicants via mobile phone. In its decision, the Data Protection Board ruled that the practice whereby the creditor identifies the loan applicants solely on the basis of the name, social security number, address and telephone number data provided via a text message that is accepted as a loan application, cannot be considered as a sufficiently reliable practice. Therefore, the Board prohibited the respondent, who followed an authentication process commonly used in the sector, from processing personal data in the aforementioned manner. The respondent lodged an appeal against the decision of the Data Protection Board to the relevant appeal court. Partly due to this case, a proposal to enact a general law on authentication was put forward in Finland. The overall reform of legislation on consumer credit was implemented with the amendment of chapter 7 of the

Consumer Protection Act (Kuluttajansuojalaki 38/1978) which entered into force on 1 February 2010.

C. Major specific issues

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

As examples of the principle of accountability, there is a requirement to produce a data balance sheet in special laws and statutes. For example, according to subsection 1 of section 2 of the government decree on ICT Agency (HALTIK) (Valtioneuvoston asetus Hallinnon tietotekniikkakeskuksesta 810/2007), the ICT Agency must annually report significant issues pertaining to processing of data within its mandate to the Ministry of the Interior and the Office of the Data Protection Ombudsman, by the end of April. The decree entered into force on 1 March 2008.

According to section 60, the Act on the Population Information System and the Identification Services of the Population Register Centre (Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 661/2009), the Population Register Centre must provide a detailed report on the processing of data and event information stored in the log register at least once a year. The act entered into force on 1 March 2010.

Surveys conducted
During the year under review, the Office of the Data Protection Ombudsman conducted several surveys.

During summer 2009, the Office of the Data Protection Ombudsman implemented a sector-wide survey on market and opinion polls. Questionnaires sent to a hundred companies charted procedures pertaining to polls and the extent of personal data processing. Particular attention was paid to the upholding of civil rights. The sector survey showed that some of the market and opinion poll makers know the requirements of data protection legislation, and take them into account in their activities. However, some of the answers demonstrated a lack of knowledge with regard to data protection requirements. Citizens' names and contact information are acquired for research purposes, especially from electronic directory and directory inquiry services, as well as official registers.

The Office of the Data Protection Ombudsman conducted a large inspection which focused on the national register of the Employment and Economic Development Offices. The Employment and Economic Development Offices have 200 outlets all over Finland. Individual clients are offered services for job seeking, career planning, occupational rehabilitation and entrepreneurship. The Employment and Economic Development Office also gives advice on applying for unemployment benefits and supports access to employment in different ways. The purpose of the inspection was to see if the processing of personal data in the national register was done according to the legislation. The inspection led to a number of conclusions, which were submitted to the Ministry of Employment and the Economy. The Ministry made several amendments and other measures on the basis of the inspection.

Since, in Finland it is possible for the Data Protection Board to issue a permit to process personal data and set special conditions for processing, the Office of the Data Protection Ombudsman conducted a survey on how well permit recipients followed permit decisions and their conditions. The survey results showed that permit conditions are followed well.

France

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

France transposed the European directive of 24 October 1995 with the law of 6 August 2004, which amended the law of 6 January 1978. An initial implementing decree adopted on 20 October 2005 was amended on 25 March 2007, with a view to incorporating the necessary procedural changes.

B. Case law

Court of Cassation decision of 8 December 2009 concerning whistleblowing

In a decision dated 8 December 2009, the social division of the Court of Cassation recalled that the scope of the whistleblowing authorised by the National Commission for Information Technology and Civil Liberties (the CNIL) within the framework of Single Authorisation No. 4 must be restricted.

This decision does not challenge the actual principle of whistleblowing schemes and clarifies the interpretation difficulties encountered by courts.

In order to comply with the requirements of the United States' Sarbanes-Oxley Act, the company Dassault Systèmes introduced a "code of business conduct" setting out the rules that employees must observe in the course of their work. A notable feature of this code is a whistleblowing system that enables employees to report any violation via a dedicated e-mail address. Prior to implementing the system, Dassault Systèmes produced a statement of compliance with Single Authorisation No. 4.

In the dispute proceedings resulting from this whistleblowing system, the Court of Cassation recalled that the scope of the Single Authorisation must be restricted. The Court clearly stated that as the implementation of a professional whistleblowing system is subject to compliance with the Single Authorisation, it must be limited to the areas of accounting, finance and anti-corruption.

Indeed, Article 3 of the CNIL's Single Authorisation No. 4 made provision for the taking into account of facts outside of that scope that affect "the vital interests of the organisation or the physical or moral integrity of its employees". The Court of Cassation specified that said article must not be interpreted as permitting a broadening of the purpose of whistleblowing schemes as provided for by the Single Authorisation. Whistleblowing systems that do not strictly comply with the conditions of Single Authorisation No. 4 must be subject to specific authorisation to be granted by the CNIL on a case-by-case basis.

Moreover, the Court of Cassation stressed the need for companies to inform the persons concerned, in accordance with the provisions of the French Data Protection Act. On this point, the decision reiterated that "the information measures provided for by the law of 6 January 1978 and contained in the Single Authorisation decision must be stated in the document establishing the whistleblowing procedure". Indeed, in the Dassault case, this information was incomplete, as it involved rights of access, correction and objection.

The CNIL is soon due to amend its Single Authorisation in light of the decision rendered by the Court of Cassation and observations made during recent audits of companies.

C. Operation and activities of the CNIL

Adoption of resolutions

In 2009, the CNIL was in session 48 times for 35 plenary sessions and 13 dispute sessions.

These meetings led to the adoption of **719** resolutions, an increase of 22.7% compared with 2008.

In 2009, the CNIL adopted:
- **544** authorisations (+**39%** compared with 2007);
- **5** authorisation denials;
- **35** recommendations on the processing of sensitive or high-risk data.

Since the introduction of the law of 6 August 2004, the CNIL has had disciplinary powers that give it the right to

impose fines of up to €150,000 (€300,000 in the event of a repeat offence), with a cap of 5% of turnover.

In 2009, the CNIL issued a total of:
- **5** financial penalties;
- **4** warnings;
- **90** formal notices.

Referrals

The CNIL received 6,482 referrals in 2009

In 2009, 4,265 complaints regarding breaches of the French Data Protection Act and 2,217 requests for indirect access rights were received by the CNIL. This reflects a slight decrease (-11.8%) compared with 2008 (2,516 requests).

Database notifications were also slightly down in 2009: 68,185 compared with 71,990 in 2008, a reduction of around **5%**.

Inspections

2009 confirmed the growing importance of inspections in the work of the CNIL, both with regard to the number of inspections conducted and the increasing variety of sectors inspected. The CNIL has implemented new procedures to respond to developments in case law relating to its activities.

First of all, some figures. **270 inspections** were conducted in 2009, **an increase of nearly 24%**. The consistent increase in the number of inspections carried out is not a new phenomenon and reflects the CNIL's wish to fully embrace the philosophy of the 2004 law that favours the on-site inspection of databases, which benefits the people whose data is being processed.

The largest proportion of inspections (31% of all inspections conducted) are performed within the framework **of the annual inspection programme** adopted by the plenary session. The 2009 inspection programme was largely kept to.

Highlights of 2009

a. The CNIL reaches maturity

2009 was marked by several parliamentary initiatives aimed at amending the French Data Protection Act.

It is worth mentioning, in particular, the fact that at the end of 2008, the Senate's Laws Committee entrusted to Senators Anne-Marie Escoffier and Yves Détraigne **a reflection on respect for privacy in the era of digital memory**.

The recommendations they made in their information report have been partly translated into a bill that was examined by the Senate in March 2010. Firstly, this bill envisages increasing the effectiveness of the right to erasure of data by strengthening the obligation to provide information about the data retention period and facilitating the exercise of the right of removal, especially on the internet. On this subject, the Secretary of State for Forward Planning and Development of the Digital Economy, Nathalie Kosciusko-Morizet, also launched, in November 2009, an extensive public consultation on the right to erasure of data, the main aim of which is to identify best practices and draft a charter for their implementation.

Moreover, the bill aims to make Information Technology and Civil Liberties Correspondents compulsory when a public authority or private organisation processes personal data, when more than fifty people have direct access to said data or are responsible for its handling.

The intention is also to strengthen the inspection and disciplinary powers of the CNIL, as well as to increase its possibility to act before the courts. Finally, the bill presented to parliament aims, *inter alia*, to specify the obligations of the data controller in the event of a violation of the integrity or confidentiality of personal data and to change the way police records are managed.

i. The strategy of openness

The Rights Protection Ombudsman

The Rights Protection Ombudsman (*Défenseur des Droits*) established by the constitutional reform of 23 July 2008 is due to become a member of the CNIL. The Ombudsman will be able to participate, either in person or through a representative, in the discussions of the Committee in an advisory capacity (Article 9 of the draft organic law). The CNIL will, therefore, be made up of 18 commissioners.

The Chairman of the CNIL is delighted about the forthcoming addition of the Ombudsman to the CNIL, which will enhance protection of the rights and freedoms of our citizens.

Increase in hearings and international openness
In a move to achieve greater international openness and improve understanding of the government's projects, the technologies and service offers currently being developed and/or current and future challenges, the CNIL organised more than 20 hearings during its plenary sessions in 2009.

In particular, members of the government were heard, namely: Nathalie Kosciusko-Morizet, Secretary of State for Forward Planning and Development of the Digital Economy and Eric Besson, Minister of Immigration, Integration, National Identity and Cooperative Development. Companies such as St Gobain, PSA, Air France and IBM were also heard by the CNIL.

In plenary sessions dedicated exclusively to international issues, the Chairman of the United States' Federal Trade Commission was also received by the CNIL in October 2009. In addition, within the framework of international cooperation, the CNIL regularly welcomes foreign delegations from around the world on study missions in France and/or Europe to share its experience regarding data protection and the organisation and powers of its supervisory authority. Thus, in 2009, the CNIL had the pleasure of receiving delegations from China, Russia (on two occasions), Indonesia, Armenia and, finally, Turkey, in order to exchange ideas about issues including digital signatures, police records, access to information, cybercrime and e-government.

Finally, in 2009, the Chairman of the CNIL became heavily involved, particularly through the AFAPDP (Francophone Association of Data Protection Authorities), in starting and consolidating actions to promote this positive dynamic. With the support of the International Organisation for the French-Speaking World, the AFAPDP organised the 3rd Annual Francophone Conference of Data Protection Commissioners, which took place in Madrid in November 2009. This conference offered a unique platform to the 30 delegations representing francophone countries and international organisations and was an opportunity to raise awareness and share experiences with francophone states that do not yet have any data protection legislation, as well as lay the foundations of a partnership with the Ibero-American Data Protection Network.

ii. Greater transparency
Until now, the CNIL was not authorised to disclose its opinions about bills.

Indeed, the Commission on Access to Administrative Documents (CADA) considered that the CNIL could not publicly disclose an opinion "so long as it was of a preparatory nature, that is, so long as the bill, order or decree to which it related had not been adopted". Even when it had lost its preparatory nature, the opinion of the Commission concerning "cases examined in the Council of Ministers, i.e. bills, orders and decrees", could not be disclosed. Consequently, members of parliament found themselves in a paradoxical situation: they debated matters examined by the CNIL, but could not take into account its opinion, even though they knew it existed.

The example of the HADOPI bill
On 3 November 2008, a daily financial newspaper published the opinion of the CNIL dated 29 April 2008 regarding the HADOPI bill, outside of any legal framework and despite the fact that our Commission was not authorised to disclose it. That publication revealed the CNIL's position in relation to the bill in its original version. After said opinion, the wording was extensively reworked by parliament. For example, in the preliminary bill, the High Authority for the Dissemination of Works and the Protection of Rights on the Internet could oblige access providers to filter content, which risked violating freedom of expression, which the CNIL highlighted. In the version submitted to the parliamentary assemblies, it was stipulated that only the judicial authorities could order access providers to filter content.

This situation, which forced the CNIL to be silent about its own opinions and also deprived the parliament of knowing them, is now in the past. Indeed, the law of 12 May 2009 on the simplification and clarification of the law and streamlining of procedures was the result of the initiative of Jean-Luc Warsmann, Chairman of the Laws Committee of the National Assembly, and now stipulates that: **"At the request of the Chair of one of**

the standing committees of parliament, the opinion of the Commission on any bill may be made public".

The recent legislative evolution, therefore, constitutes a major advance with regard to the transparency of the activities of the Commission and will help improve the quality of parliamentary work.

iii. The CNIL welcomed new members in February 2009
Jean-Paul Amoudry, Senator (UC) for Haute-Savoie
Jean-François Carrez, Division President at the Court of Audit
Claire Daval, Lawyer, lecturer in Public Law at Lille 2 University
Marie-Hélène Mitjavile, Councillor of State
Dominique Richard, Consultant

b. Technological expertise
The CNIL assists companies and public authorities from the stage of designing their systems. Through its advisory role and during the examination of formal files, the Commission may have to advise companies or public authorities to modify their systems, use alternative technical solutions or incorporate data protection guarantees.

In the field of health, the CNIL is on the steering committee responsible for implementing the new national health identifier, which will be the cornerstone of the future individual electronic medical record. It is also part of the committee working on the RGI (Référentiel Général d'Interopérabilité), which is a framework of recommendations describing standards and best practices to facilitate interoperability between the information systems of the public administration, published on 12 June 2009.

Moreover, following studies carried out last year on biometric devices for finger vein pattern recognition, a form of biometrics considered untraceable, in May 2009 the CNIL adopted a Single Authorisation concerning these devices when used for the purpose of controlling access to restricted areas in places of work. Palm vein pattern recognition had also been used in applications designed to combat cheating in exams.

Targeted advertising
The economic models of many leading internet companies are based on the supply of services that are seemingly "free" to the internet user, but which are mostly, if not exclusively, financed by advertising.

Targeted marketing has become the "fuel" of the digital economy, which is increasingly hungry for personal data.

These developments raise fears about systematic profiling of internet users without their knowing, as well as the risk of commodification of individual profiles among content providers and advertisers.

In its report, which was made public in March 2009, the CNIL looked at the various online advertising techniques, the risk of privacy violations and possible countermeasures.

Nanotechnologies
In its warning and advisory role, the main task of the CNIL is to ensure that the development of new technologies does not violate human identity, human rights, privacy or civil liberties.

The main challenges linked to the growth in nanotechnologies lie in the difficulty of controlling something that cannot be seen and detecting the risks that they pose, particularly in terms of the traceability of people and the right to privacy.

How can we ensure that we are informed of the existence, purpose and effects of an invisible (or nearly invisible), dispersed technology? How can we ensure that the development of these technologies will not give rise to "hyper traceability" of people, jeopardising their freedom to come and go? Because this freedom does not exist if anonymity is not guaranteed!

In the face of these challenges, it is essential to consider how this area should be regulated, as well as a possible evolution of the legislative framework. In particular, should certain uses of nanotechnologies be banned?

It is also important to identify which rules to promote for the protection of individuals. The principles of no harm, proportionality, safety, information and individuals' control over their personal data are guarantees that need to be integrated upstream, at the stage of designing nanotechnology systems and applications.

That is why the CNIL actively participated in the large national public debate on nanotechnologies, with the aim of raising the awareness of individuals and public authorities to the risks inherent in these technologies. One of its main activities was the drafting of a "Stakeholders' Guide" summarising its questions.

Standardisation
In 2008, the CNIL teamed up with GCSSI, the group in charge of the standardisation of safety at AFNOR (the French Standardisation Association), with the aim of positioning itself as a central standardisation actor in key areas of data protection. This group prepares the French positions on draft ISO standards.

ISO is currently developing draft standards for the protection of privacy and personal data. Since 2005, it has been working on a draft standard called ISO 29100 "Privacy Framework", which establishes common requirements and a common terminology for privacy protection at international level. It is a founding document that could eventually serve as a reference for other standards.

As the structure and principles of this draft standard appear less stringent than and often in contradiction with European standards, the Chairman of the CNIL urgently mobilised WP29 and the European Commission on this matter in June 2009. WP29 gave this matter its full attention and the CNIL coordinated the preparation of comments with its European counterparts, as well as with its industrial and institutional contacts at AFNOR.

For the first time, in November 2009, a CNIL representative participated in one of the biannual international meetings of the group responsible for preparing this standard at ISO. ISO highlighted its interest in receiving contributions from data protection authorities and expressed its wish to formalise a "link" with WP29.

Moreover, ISO decided to set up a Privacy Steering Committee (PSC) in order to better coordinate its activities in the field of privacy. Aware of the strategic, cross-cutting importance of this Committee, the CNIL has managed to have one of its representatives included in the list of experts on the PSC, the first meeting of which will take place in February 2010.

Audits of electronic voting systems
During 2009, the CNIL audited electronic elections organised by private organisations and ministries (industrial tribunal and College of Nurses elections). These audits were also an opportunity to check the voting systems offered by the different service providers in the market.

In particular, the CNIL checks the physical and logical locks of the electronic ballot box, in order to detect any modification of the voting device and prevent any manipulation of votes. It examines whether or not there is any way of connecting to the voting device during the ballot. It then checks whether the different programmes comprising the voting device have been fully assessed, taking copies of documents and computer databases as permitted by law. Finally, the Commission examines the steps taken to verify the identity of voters and ensure the secrecy of votes.

These audits revealed the inadequacy of the guarantees provided by the voting devices in terms of data security and confidentiality.

Consequently, the Commission took disciplinary action against several organisations that had carried out electronic elections because it considered that certain important points of its recommendation had not been implemented.

c. The STIC audited and criticised
The STIC is a national database that records information gathered from proceedings brought by the police force within the framework of criminal investigations. Its purpose is to *"facilitate the detection of criminal offences, the gathering of evidence of those offences and the search for their perpetrators, as well as the use of data for statistical research purposes"*.

However, this database has also become an administrative investigation tool as, since the introduction of the law of 21 January 1995 on guidance and planning in relation to security, it can be consulted in relation to the recruitment, accreditation or security clearance of members of a wide range of professions. This applies, for example, to surveillance and security personnel, people wishing to work in airports, municipal police officers, prefects, ambassadors, magistrates, and so on. In total, it is likely that STIC consultations for administrative investigation purposes concern more than a million jobs.

The CNIL expressed its opinion on the successive laws passed to manage this database and, on that occasion, was able to share its observations[18]. Moreover, the daily work of the CNIL involves performing checks requested by the interested parties themselves within the framework of indirect access rights. Additionally, in 2009 it carried out a complete audit of the database, making it possible to thoroughly assess the operation of the STIC.

Thus, numerous on-site inspections have been carried out (in police stations, regional criminal investigation departments, courts, prefectures, etc.) in order to verify on site the procedures for feeding the database, the conditions and effectiveness of its updating, access rights and existing security measures.

The results obtained are rather worrying and reveal that this database is not updated regularly. Indeed, it appears that in 2007, only 21.5% of cases closed due to lack of charges or an insufficiently established offence, 31.17% of discharge decisions, 6.88% of acquittals and 0.47% of case dismissals were notified for updating of the STIC.

The CNIL formulated **11 proposals** to improve control and security in the use of the database, in order to improve the accuracy and updating of the information recorded and widely consulted.

d. Databases used in immigration matters

Beyond the political controversies in this field that marked 2009, the databases used within the framework of the administrative management of foreign nationals underwent a number of changes.

The OSCAR database

A new database called OSCAR, provided for by the law of 20 November 2007 on controlling immigration, integration and asylum, was created in 2009. It is a biometric database that records the fingerprints of the beneficiaries of an assisted return scheme, that is, foreigners living in France who choose to return to their country of origin in exchange for financial assistance. The CNIL has asked that the biometric data of these foreign nationals be deleted from the database if they are not accepted into the scheme and that said data only be used for the purpose of determining whether they have already received this assistance.

RMV2 (Worldwide Visa Network)

A complete overhaul of the RMV 2 system, which records visa applications, has been commenced. This overhaul must make it possible to implement the ***VIS*** (Visa Information System, which will pool information about Schengen visa applicants between European states), while also extending access to this information to prefectures, customs authorities and even some members of the police force. It is also envisaged that external service providers will be used to collect visa applications and record the corresponding information in the system, a point on which the CNIL has expressed serious reservations, given the possibility of this data being used by those service providers or the authorities of the countries in which the visas are issued.

GIDESE and FNAD (entry-refusal database)

Two other databases were introduced in 2009, on a trial basis. The GIDESE database is designed to monitor the movements to and from Réunion Island of foreign nationals in possession of a visa, in order to enable the authorities to locate people staying on the island illegally.

FNAD (entry-refusal database) is a biometric system that records the fingerprints and photographs of foreign nationals found not to fulfil the necessary entry conditions by the border control personnel. Created for two years in 2007 and limited to the border of Roissy airport, the Ministry of Immigration has extended the FNAD trial for a further two years. The CNIL ensured that this

[18] Resolutions No. 98-97 of 24 November 1998, No. 00-064 of 19 December 2000, No. 2005-187 of 8 September 2005.

trial was rigorously assessed, in order for the usefulness of this database, which would only make it possible to identify persons violating the rules of entry into French territory on more than one occasion, to be more clearly established before possibly being rolled out throughout the national territory.

Records concerning asylum seekers

The CNIL is particularly attentive to the evolution of these databases, which must be subject to specific guarantees, given that asylum applications contain highly sensitive data such as applicants' ethic origin, political opinions and religious beliefs.

This year, the Ministry of Immigration created the DN@ database, which is intended to improve the management of the accommodation capacity of centres for asylum seekers. It records information that enables the individualised tracking of the persons admitted to the centres. On the recommendation of our Commission, the DN@ database does not record any data concerning the social protection or health of the individuals in the centres, which is not necessary for administrative capacity management. It also demanded that the recipients of the information (particularly the French Immigration and Integration Office (OFII), the asylum services of the Ministry of Immigration and prefectures) are all subject to an individual designation and clearance procedure, to ensure that only the agents directly involved in receiving asylum seekers have access to the information recorded in the DN@ database.

The use of databases containing information about asylum seekers is not limited to the administrative authorities. Indeed, this year the CNIL authorised CIMADE, an organisation that defends the rights of foreign nationals and works in immigrant detention centres, to create two computerised databases designed to manage the applications of the foreigners it assists at both its own centres and at the detention centres. CIMADE has proven particularly attentive to the security measures surrounding the operation of these databases (data access rights, traceability of actions, etc.), the information retention period, which may not exceed one year, as well as arrangements for informing individuals and their exercise of the rights of objection, access and correction or removal of data concerning them.

Germany

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

On 1 September 2009, several important amendments to the Federal Data Protection Act entered into force. As a reaction to the wave of data protection scandals in the private sector, which started at the beginning of 2008, the rules on data processing by third parties and the use of address data for advertising purposes were tightened. In addition, the data protection authorities were given broader powers to impose sanctions in the non-public sector. For the first time, they obtained effective means of action and are now in a position to have controversial issues of interpretation clarified by judicial intervention. Mandatory notification in the case of data protection breaches is also a new rule: Private companies are obliged to notify data subjects and the respective data protection authority in cases of serious violations of data protection rules. Finally, lawmakers have created specific provisions on the collection, processing and use of employees' data which also includes paper files and handwritten records. However, this regulation does not constitute comprehensive regulation of all forms of handling employee data; however, according to Federal Government plans, such a regulation is to be developed in 2010.

B. Major case law

Prolongation of the Federal Constitutional Court's provisional orders on data retention for later use
In its decisions of March and October 2008 (file number 1 BvR 256/08), the Federal Constitutional Court provisionally restricted the use of data stored according to the "Act on the new regulation of surveillance in telecommunications and other covert investigative measures and on the implementation of Directive 2006/24/EC". In this way, the Federal Constitutional Court restricted the number of crimes for which data may be retained to a catalogue of serious crimes and it limited the purposes for the use of data for averting dangers and for the purposes of intelligence services to cases in which there is an imminent threat to a persons' life, limb and liberty, to the existence or security of the Federation or of a Federal State or if the use of data is necessary for averting general danger. As the decisions were respectively restricted to six months or alternatively until the Court's ruling on the main issue, in 2009, they were pertinently prolonged by the Federal Constitutional Court without any further amendments of the content. A decision is expected in relation to the principal proceedings in 2010.

Decision of the Administrative Court in Berlin to release providers from mandatory data retention, repealed by the Higher Administrative Court of Berlin-Brandenburg
By provisional order, in October 2008, the Administrative Court in Berlin prohibited the regulatory authority (Federal Network Agency) from fining providers that refused to fulfil their obligation of data retention. The reasons given by the Court for its rulings were that the provisions on compensation for the telecommunications providers' technological and personnel investments needed for data retention, were not sufficient. The Federal Network Agency lodged an appeal against these decisions with the competent Higher Administrative Court in Berlin-Brandenburg. Contrary to the Administrative Court, this Court decided on 2 December 2009 that, in any case, the doubts which exist in relation to costs for setting up the technical framework to allow the retention of data are not of such a nature as to waive the obligation of telecommunication companies for compliance with compulsory Community law..

C. Major specific issues

Visa warning data file
The Federal Government elected in 2009 intends to resume the legislative project on a visa warning data file in a reduced form. In the previous legislative period, this project failed. With regard to this project, a central critical point relating to data protection law,, raised against this project in the last legislative period, shall be taken into consideration. The Federal Government's intention is that data on inviting parties and on signatories of the formal obligation to the immigration authority shall only be registered if they were identified with illegal behaviour in connection with the visa-granting procedure or in reference to a foreign country.

However, as regards data protection law, there are still doubts regarding the envisaged regulation. In particular,

the real requirement and the long-term existence of a "separate national solution" against the backdrop of the European Visa-information system (VIS) seem to be doubtful. In addition, there is still a need for clarification of the setting up of the Visa warning data file and the access rights to the stored data.

Adaptation of the Act on the central register of foreign residents (AZR-Act)

As a consequence of the ruling of the European Court of Justice on the *Huber* case (ruling of 16 December 2008, case C-524/06) the Act on the central register of foreign residents has to be adapted. The new legal regulation has to ensure that the only data stored in the register on EU citizens is that which is absolutely necessary for the application of the provisions related to the right of residence.

Moreover, the purpose of the data stored in the central register of foreign residents must be strictly limited. Therefore, from a data protection point of view, access of law enforcement authorities to EU citizens' data in the framework of a so-called "overlapping of tasks" (data are collected for different tasks and are available to different authorities for their tasks) is critical if there is no guarantee that data which has been collected and processed is exclusively used for purposes related to the right of residence.

Adoption of the Gene Diagnostics Law

On 24 April 2009 the German Bundestag adopted a law on gene diagnostics regulating genetic examinations for medical purposes, for the clarification of parentage and of issues related to the insurance sector and working life. In addition, the law regulates the handling of genetic data. Among the most important basic principles of the draft is the individual's right to informational self-determination. This includes both the right to know one's own genetic medical results and also the right to ignore them (the right to not know).

Only a doctor of medicine is allowed to carry out a genetic examination for medical purposes. In this respect, advice to patients is essential. If an examination leads to a prognosis of a risk of disease (predictive gene diagnostics), advice on genetics prior to and after the examination is mandatory.

A genetic examination for finding out parentage is only admissible if the persons whose genetic sample is to be examined have given their consent to the examination.

With regard to labour law, it is particularly forbidden to carry out genetic examinations at the request of an employer. An employer is not permitted to request the results of a genetic examination that has already been carried out, and is not entitled to receive them or use them. However, as regards safety at work, genetic examinations may be allowed in exceptional cases and under strict conditions in the framework of preventive medical check-ups for workers.

Insurance companies are not permitted to request genetic examinations or the disclosure of results from genetic examinations that have already been carried out, or receive or use such results or data, before or after entering into an insurance contract. There are some exceptions subject to strict limitations: when entering into contracts for life assurance, disability insurance, occupational disability insurance and nursing care insurance, the results of genetic examinations that have already been carried out must be presented if a benefit exceeding 300,000 euros or an annual income amounting to more than 30,000 euros is agreed upon.

Unfortunately, there is a lack of regulation on the handling of genetic examinations in connection with research.

Greece

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

A number of legislative developments took place in 2009 related to the national legal framework on personal data protection. Recently, the Minister of Justice, Transparency and Human Rights of the new government announced that the amendments made last summer to the national data protection act (see point 1, below) and to the Penal Code (see point 3, below) will be revised, according to the corresponding opinions of the Hellenic Data Protection Authority (HDPA) (see Opinion 1/2009 and Opinion 2/2009, below).

1. Amendment of the Greek data protection act 2472/97 with respect to CCTV systems in public areas

A new amendment was made to the Greek data protection act, 2472/1997, and more specifically to Article 3, i.e. the scope of application of the law. Accordingly, the law does not apply to the processing of personal data that is carried out by the relevant public authorities through the use of special technical devices for the recording of sound or images in public spaces with the aim of safeguarding the security of the state, national defence, public security, the protection of persons and property and the management of traffic. The material collected through such devices (as long as it does not fall under point b of the present article[19]) is stored for a period of 7 days, after which it is destroyed at the order of the public prosecution authority. Any breach of the above provisions shall be punished by imprisonment for a period of at least one year, unless a stricter punishment is provided for in any other law.

According to the report accompanying the above provision, the introduction of the aforementioned exception is considered necessary in light of the high rise in crime and the methodology employed by the perpetrators of crime.

2. New law imposing identification of subscribers, users and technical equipment in the sector of mobile telephony

The new Law 3783/2009, published in August 2009, puts an end to the anonymity of subscribers (and users) of pre-pay mobile phones for the purpose of national security and the investigation of serious crimes. For the same purposes, irrespective of the type of contract, it imposes registration obligations on a) the technical equipment of mobile phones of subscribers and users and b) the users' identification data (i.e. where a subscriber pays for a series of mobile phone numbers used by other people, i.e. employees).

[19] The provisions of this law shall not apply to the processing of personal data which is carried out by:
a) a natural person in the course of a purely personal or household activity.
b) judicial-public prosecution authorities and authorities that act under their supervision in the framework of attributing justice or for their proper operational needs with the aim of verifying crimes that are punished as felonies or misdemeanours with intent, and especially with the aim of verifying crimes against life and against sexual freedom, crimes involving the economic exploitation of sexual life, crimes against personal freedom, property, and the right to property, violations regarding drugs, plotting against public order, and crimes against minors. With respect to the above, the existing material or penal procedural provisions apply. During the exercise by the citizens of their right to assembly, pursuant to article 11 of the Constitution, the use of sound or image recording devices or other special technical means is allowed under the conditions referred to in the next item.
The recording of sound or image through any technical device with the aim of verifying the commitment of the above mentioned crimes is allowed at the order of the public prosecution authority and provided that public order and security are at serious risk.
The sole aim of the aforementioned recording is its use as evidence for the commitment of crimes before any investigative authority, public prosecution authority or a court of law. The processing of any other material that is not necessary for achieving the aforementioned aim for the verification of committed crimes is prohibited and the relevant material shall be destroyed at the order of the competent public prosecutor.

More specifically, providers have to collect personal data related to identification from current and new subscribers and users. As far as the current subscribers are concerned, this had to be completed by 30 June 2010. If a subscriber failed to submit their identification data to the provider by 30 July 2010, then the provider must proceed with the disconnection of the specific subscriber from the service. Providers have the obligation to retain the data for up to a year after discontinuation of the subscription, which should be at no extra cost to the subscriber.

Identification data that needs to be collected from the subscriber includes name, father's name, place and date of birth, photocopy of national ID card or passport and the national taxpayer registration number. The categories of data are slightly different for subscribers that are legal entities. Further data needs to be collected for the identification of the mobile equipment, such as the IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity) numbers, as well as the time and place (cell-id) of the first activation. Every SIM (subscriber identity module) card sold has to be paired with an identified subscriber. The subscribers are obliged to notify the provider in writing of any changes of use to the pre-pay mobile phone, such as loss, theft, or any transfer of the SIM to another person.

Access to the data retained by the provider will be available only to the law enforcement authorities according to the law on lawful interception of communications. Currently, according to recent estimates, there are 13.5 million anonymous pre-pay mobile phone subscriptions in Greece, of which 9 million are active connections. Only 5 million are registered (i.e. the subscriber is identified).

3. Amendment of the Greek Penal Code with respect to DNA analysis and the creation of a database of DNA profiles

Article 200[A] of the Code of Criminal Procedure was recently amended as follows (amendments appear in italics):

1. *"When there are serious indications that an individual has committed a felony or a misdemeanour which is punishable by imprisonment of at least three months, law enforcement authorities shall collect a cellular sample for DNA testing in order to determine the identity of the offender."*

   The analysis is restricted solely to the data necessary to identify the offender and takes place at a state or university laboratory.

   The accused is entitled to his/her DNA analysis for his/her own defence.

2. If the aforementioned analysis proves to be conclusive, the result shall be announced to the person to whom the cell sample belongs, and he or she shall have the right to ask for a re-analysis. In that case, the provisions of Articles 204 to 208 shall apply. The investigating officer or the public prosecutor shall also have the right to ask for a re-analysis. If the analysis proves to be negative, the cell sample and the DNA profile shall be immediately destroyed. If, however, the analysis proves to be positive, the cell sample shall be destroyed immediately. Nevertheless, the DNA profile of the *person who is accused of the offence, shall be kept in a special database maintained by the Criminal Investigation Department at the Hellenic Police Headquarters. This data is kept so that it can be used in the investigation of other offences and shall be destroyed in all cases after the death of the person involved. The operation of the database shall be supervised by a deputy public prosecutor or a chief public prosecutor who is appointed by the Supreme Judicial Council, in accordance with law, for a two-year term of office.*

3. *The destruction of the cell sample and DNA profile referred to in paragraph 2 shall take place in the presence of the judicial officer who supervises the operation of the database*. The person to whom the cell sample belongs is asked to be present during the destruction of his/her sample and he/she may be accompanied by counsel and a technical expert."

B. Major case law

Opinion 1/2009 - on the amendment of the Greek data protection law with respect to the operation of CCTV systems in public places (see above-mentioned amendment of Law 2472/1997)

Having considered the Constitution, the European Convention on Human Rights (ECHR), and Convention 108 of the Council of Europe, and having carried out a comparative overview of the relevant law in other EU Member States, the Hellenic Data Protection Authority issued the opinion that:

- The provision in question practically excludes the operation of the devices of sound/image recording in public places from the scope of application of L. 2472/97 and from the supervision of the HDPA. In this sense, the provision does not fulfil the quality requirements set by the jurisprudence of the European Court of Human Rights concerning any law that introduces restrictions on a fundamental right. More specifically, the submitted amendment scores low in terms of the predictability of its consequences, because it does not specify the conditions and procedure for the data processing in a way that would provide the subjects of this data with adequate guarantees against arbitrary action. Furthermore, from a law-making point of view, the provision should be part of the law regulating the public authorities which will act as controllers.
- The general invoking of the protection of public security does not fulfil the requirement of specificity. There should be further clarification of the reason for the data processing. For example, one such legitimate formulation of it would be the deterrence of crimes against life, personal freedom and property. Unless such aim is specified, it is impossible to verify whether the principle of proportionality (as formulated within the Greek Constitutional System and the ECHR) has been respected, whether, that is, the specific intervention of public power in private life (video surveillance of public places) and the restrictions imposed thereby on the right to personal data protection is necessary and suitable for achieving its intended purpose.
- The provision does not specify the criteria of danger (high crime rate in an area/buildings which may need special protection) on the basis of which it will ultimately be decided whether the installation and operation of CCTV in public spaces is necessary or not. Consequently, the decision regarding the place and time of the installation of CCTV is left to the absolute discretion of the competent authorities. Any such unlimited discretion, however, exceeds the necessary measure, which, according to the jurisprudence of the European Court of Human Rights and the Greek Council of State, justifies the imposition of restrictions on human rights. In this particular case, there is a danger of unlawful infringement not only of Art. 9A of the Constitution, but also of other constitutional rights (Art. 2 par. 1, 5 par. 1, 11).
- Besides the time limitation for the storage of this data, there are no specific rules for the collection, storage, use and further transmission of the data. This omission raises serious concerns regarding the adequacy of the amendment in terms of its conformity with the quality requirements set out by the European Court of Human Rights regarding the interference to the right to private life (Art.8 of the ECHR).
- There is no provision for the organisational and technical measures required for the security of the collected and stored data.
- There is no provision for the effective protection of the data subjects' rights which may be infringed upon by that data processing. Such a safeguard, however, is part of the very core of the constitutional right to the protection of personal data. (Art. 9A of the Constitution).
- It is not clearly defined who the controller of said data will be. The general reference to the "competent public authority" does not sufficiently protect the individual in case of an infringement of the provision. Furthermore, the provision creates the risk of a potential conflict of competencies between the different Authorities involved.
- There is no requirement that the installation of CCTV is grounded upon a prior administrative act. This means that the judicial review of any such installation cannot be very effective. The only thing that the offended individuals (those whose data has been registered even though they have not been involved in any criminal activity) can do is file a lawsuit for compensation against the state.
- Last but not least, the exclusion of a wide and sensitive sector of state action from the scope of competence of the HDPA infringes the very core of Art. 9A of the Constitution and it could be argued that it is not consistent with Art. 8 par. 2 of the ECHR as this has been interpreted by the European Court of Human Rights. The wording of Articles 9A and 101A of the Constitution, as well as the Parliament's discussion relating to the adoption of these provisions in 2001, indicate that the lawmaker conceived the set-up and

operation of the DPA as a necessary institutional warranty for the protection of personal data. The need to set up an independent authority with all the necessary technical know-how stems from the fact that the rapidly evolving IT developments pose a threat to the protection of privacy. Hence, the supervision of the HDPA in the area of data processing in the public and in the private sector is part of the very core of the fundamental right to informational self-determination.

In conclusion, the amendment is merely excluding the operation of the devices of sound/image recording in public places from the scope of application of L. 2472/97 and from the competence of the HDPA and, therefore, it does not conform to Article 9A of the Constitution and Article 8 of the ECHR.

Opinion 2/2009 - on the amendment of the Penal Code with respect to DNA analysis and the creation of a database of DNA profiles

The main observations are as follows:

- Although the amendment has some positive features, it does not meet all the qualitative ones required for establishing the human right to the protection of personal data, especially in the case of DNA profiles used for the purpose of crime detection.
- In order to observe the principle of proportionality, especially its aspect of necessity, it should be stipulated in the law that genetic analysis shall only be permitted if there is no other means of evidence capable of identifying the offender.
- The list of offences in relation to which the use of DNA profiles as part of the investigation is permitted has been expanded, and now includes all felonies and misdemeanours which are punishable by a prison sentence of at least three months.
- It is necessary to differentiate, based on qualitative criteria, between the investigation of an actual current offence and the future investigation of other offences (the latter shall be enabled by the set-up of a DNA profiles database). In order to limit the use of DNA profiles with a view to ensuring the principle of proportionality, the legislator should consider either limiting the list of offences to felonies for the actual and future investigation or b) permit the use of DNA profiles for the actual investigation of all felonies and misdemeanours. However, in the case of storage of DNA profiles for future use, this should only be permitted for the investigation of very serious offences e.g. felonies and/or offences that violate specific legal interests, for instance sexual freedom (even though the latter may fall under the category of misdemeanours). Should the second solution be preferred, every in concreto judgment should be based not only on the severity of the offence, but also on other criteria concerning the offender himself (previous life, personality, etc.), which may establish the likelihood that he will re-offend (negative prognosis).
- The amendment does not make any distinction regarding the storage of DNA profiles of convicted and acquitted persons, or adults and minors. Moreover, such storage may last for an unlimited period of time (the only time limit is the death of the suspect). The above-mentioned problems can be addressed as follows: a) the DNA profiles of those who have been irrevocably acquitted for whatever reason should be removed from the database of DNA profiles; b) the DNA profiles of those who have been irrevocably convicted may only be stored for a limited period of time after their sentence has been served; c) the DNA profiles of minors below the age of 13 to whom only reformative and rehabilitation measures may apply, shall not be stored; and d) the DNA profiles of minors over the age of 13 who have been irrevocably convicted may be stored for a specific period of time, significantly shorter than that applicable to adults.
- There is no protection of unidentified DNA profiles.
- As far as the database of DNA profiles is concerned, a law or presidential decree relating to the powers and the structure of the Hellenic Police should make provisions, among other things, for the following: a) the aim of the transfer and online access to DNA profiles, which should coincide with the aim for which the initial storage is allowed; b) the public authorities that have access to the database or to which transfer is allowed; c) the rights of access and objection of the data subjects, including the obligation of the data controller to inform the data subjects about the operation of the database and that their profiles will be stored in said database; d) the deletion and blocking procedures that are in place in those cases in which the data is not deleted; e) the appropriate measures for the security of the database, prevention

of non-authorized access, modification and transfer of the data, and monitoring of every intervention.

- The amendment repeals the role of the judicial council as a procedural safeguard for the obtaining and analysis of cell samples and, in doing so, downgrades this process to a simple act of investigation. Since, however, obtaining (and analysing) a cell sample constitutes a particularly invasive interference which requires the clarification and specification of vague legal concepts (i.e. serious indications, negative prognosis), a judicial guarantee should be provided for either by a judicial council decision or at least by a prosecutor's order that has specifically been issued for this reason.
- The database of DNA profiles should be supervised by a deputy public prosecutor or a chief public prosecutor. The public prosecutor undoubtedly constitutes an additional institutional guarantee. If, however, this were to be considered as an alternative to the supervision exercised by the Data Protection Authority, this would go against the core of Article 9A of the Constitution, which clearly stipulates that the DPA provides an institutional guarantee of the human right to personal data protection.

In conclusion, the amendment should be modified along the lines of the above observations in order to be fully harmonised with the requirements of Article 9A of the Greek Constitution and Article 8 of the European Convention of Human Rights.

Decision 75/2009 - on the creation of a database containing the practising members of the Athens Medical Association, accessible on the web

- In the case in question, the request of a company concerned the collection of the personal data of practising members of the Medical Association from the website of the association (which is a public body) in order to create a new web portal with the purpose of providing individuals with a simplified search to find doctors according to their speciality and geographic categories, as well as other additional criteria (e.g. doctors contracted to specific health funds). The members of the Medical Association were notified before the disclosure of their data to third persons or on the website of the Association, so that their data could be disclosed for purposes such as informing the public and promoting scientific collaboration, and they have been given the right to object.

  The Hellenic DPA decided that the secondary processing purpose is different from the primary one (register of doctors to inform the general public, to aid scientific collaboration, etc.) but not incompatible, provided that the creation and operation of the new enriched database is similarly intended to inform the public.

- The re-use of public sector information for the purpose of commercial exploitation is already permitted and is not deemed incompatible with the primary purpose for which the public document was drawn up. However, the legitimate interests of the data subjects, who have communicated their personal data for a specific purpose and do not expect them to be used for a different purpose not directly related to the primary one, as is the case of the secondary purpose of commercial exploitation, should be sufficiently protected. The provisions of Law 3448/2006 on the re-use of public sector information, which incorporates into national law the European Directive 2003/98/EC on the re-use of public sector information, also apply to the re-use of information that is derived from publicly accessible sources, since in this case the derived information is still "in the possession" of the data controller.

The processing by the company is lawful under the following conditions: the data subjects are previously informed in writing and granted the right to object to the processing. The processing should be without economic costs for the data subjects and their names should appear in alphabetical order.

Decision 83/2009 – on the collection, use and trading of electronic communications data and other data

Following a significant number of complaints, the Hellenic DPA carried out an inspection at the premises of a company that provided a product called "Hellas Navigator – Golden Customer Lists". The HDPA imposed administrative sanctions for:

- Email harvesting and the selling of email addresses. The company was using larbin web crawler (initially

set up to .gr and .com.gr domain names) to collect addresses from the internet (a total of about 160,000 addresses were discovered). The address list was sold to more than 400 customers, including advertising agencies, banks, politicians, and public sector bodies.
- Data collection from professional unions' lists and exhibition guides (including email addresses) without data subjects' prior information.
- Correlation of telephone directory data published in public telecom providers' directories with geolocation data without the data subjects' consent.
- Sending spam, i.e. emails advertising its products without recipients' prior consent. Spam was sent with the use of Turbo Mailer through 4 different providers/adsl connections (sender address changed: hnv@otenet.gr, hellasnv@otenet.gr, hnv2@altecnet.gr, hnv1@hol.gr and calino1@ath.forthnet.gr)
- Selling licence rights for this database data to US governmental bodies in 2004 without notifying and obtaining a permit from the HDPA.

The HDPA issued a formal warning for the violation of the obligation to use telephone directory data for other purposes without data subjects' prior consent. For all other violations, the HDPA imposed a total fine of 65,000 euros and ordered the deletion of all email addresses kept by the company for their own purposes and those contained in the product "Hellas Navigator – Golden Customer Lists".

Decision 91/2009 – on Internet-based three-dimensional virtual street navigation services

The Hellenic DPA decided that the provision of a three-dimensional virtual street navigation service for Greek regions by the company "KAPOU S.A. GEOINFORMATICS" is considered processing of personal data insofar as the pictures contain identifiable persons, vehicle licence plates and houses. The processing conforms to Law 2472/1997, specifically on the basis of article 5 paragraph 2 part e, as the development of economic activity with benefits for the users, who are in a position to navigate places virtually, is a legitimate purpose. However, since the data subjects who are directly or indirectly identifiable from the pictures have no previous contact with the data controller which could justify any possible processing of their data, the service should be provided under the following conditions: a) people's faces and vehicle licence plates will be blurred before launching the service to the public; b) the retention period of raw data, i.e. the unblurred images, is set to six months from the image capture and, in addition, suitable technical and organisational security measures should be taken; c) additional measures should be taken relating to possible sensitive data; in particular, the data should be blurred as a priority. In addition, the data controller should grant the right of access (to the raw data) and the right to object before the publication of the service on the internet. The objections should lead to the blurring or deletion of the raw data. Following the publication of the data on the internet the data subject or any other third party can report the lack of or inadequate blurring of any face or vehicle licence plate. The blurring of a person's image can also cover a larger area of the image in addition to the face if the data subject requests this (before or after publication on the internet), as under certain circumstances the data subject may be identifiable from his/her body type. Only data subjects can request that their house be blurred. Finally, the obligation to provide information to the subject will be fulfilled not only through the marking of the equipped vehicles collecting the images but also through the press, such as newspapers, and also through the company's website in an easily accessible manner.

Decisions 56/2009 & 74/2009 on biometrics

Two HDPA Decisions with regard to the lawfulness of the processing of biometric data were issued in the second half of 2009. Both Decisions were based on the principle of proportionality. More specifically, with Decision 56/2009 the HDPA permitted a certification service provider to establish a card-based fingerprinting biometric system for access control in the specific area used for the creation and maintenance of cryptographic keys (i.e. Certification Authorities' private keys used for signing the users' qualified certificates). On the contrary, in Decision 74/2009, the HDPA prohibited the operation of a facial geometry biometric system connected to a central database as a measure controlling employees' access to the premises of a banking-related services company. In this case, the HDPA concluded that the company could make use of less intrusive measures for physical access control, whereas stronger measures

could be applied in dedicated areas where critical data was stored, together with logical access control measures in the company's technical system.

Decision 9/2009 on organisational measures in clinics

A patient alleged that he had provided an X-ray to a clinic that had been produced elsewhere for further assessment and treatment by the clinic's medical personnel. After the surgery in the clinic, because it was not successful, he asked the clinic to return the X-ray in order to submit his medical file to another clinic for further consultation and possible treatment. The clinic did not respond to his request in writing and the patient was verbally informed that his X-ray had been lost. After an inspection at the premises of the clinic, the HDPA found out that the clinic does not keep full medical records, but only some information with regard to the type of medical examinations carried out by the clinic itself as well as administrative data of the patient. The HDPA noted that there is a legal obligation to keep full medical records as laid down by the Law on Code of Conduct for Physicians. The HDPA imposed a fine to the clinic for not having formally responded to the request of the patient (i.e. violation of the right to access) and for not having applied such organisational measures that may prove whether medical data is kept and returned safely to the patient.

Hungary

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

The "data retention directive" has been fully transposed into Hungarian law. Traffic data related to successful calls are retained for one year, and in the case of unsuccessful calls, for half a year. The one-year retention period is applied for traffic data generated through internet use.

The act implementing the "data retention directive" has been challenged before the Constitutional Court. However, the Court has not yet made a decision about this matter.

B. Major case law

Camera surveillance at demonstrations
Many citizens complained about the police practice of installing cameras to monitor the participants of demonstrations held in public spaces. In his opinion, the commissioner first stressed that any actions taken by public authorities must encourage the use of fundamental rights, including freedom of expression. The use of cameras by police forces might deter citizens from participating at demonstrations. The use of these devices is only acceptable if there is a real risk of an unlawful and violent action disturbing the demonstration and intervention of police forces is necessary in order to restore order.

Computers seized by the police
A citizen stated in his complaint that his computer was seized by the police as part of criminal proceedings and he was unable to get it back for more than half a year. The Commissioner took the view that it was acceptable for police to seize IT tools if they were used to commit a crime. However, the criminal proceedings cannot cause any harm which is not necessary to carry out a proper investigation. The period of more than six months obviously exceeded the acceptable time limit that can be justified by the aims pursued by the criminal proceedings.

Access to voice records
Several citizens complained about refused requests to access voice records kept by various service providers. The requests were generally refused since there was no need for the applicant to possess the record. The Commissioner emphasised that data subjects have a right of access to information held about them which can only be restricted if explicitly regulated by law. Since there is no statutory limitation on the right of access, complainants have the right to have a copy of the conversation recorded by the service provider. This approach was confirmed by the legislator later in the year when amending the consumer protection rules clearly ensuring data subjects' right of access to the copy, including his conversation with the operator.

C. Major specific issues

In 2009, two companies started negotiations with the Commissioner with the aim of persuading the Commissioner of the necessity of the so-called positive debtors' list. Negative files related to the non-fulfilment of financial obligations already exist in Hungary and do not require the data subject's consent. Nevertheless, the collection of financial solvency information does require the data subject's consent.

The Commissioner is not in favour of setting up a credit register (positive list). According to the Commissioner, clients are under pressure to give their consent to the processing, thus the "freely given" component seems not to be ensured. There were also doubts about sufficient information being given to the data subjects. Numerous financial institutions are supporting the idea of the positive debtors' list and, despite the warnings of the Commissioner, they initiated a "pilot phase" of the project, collecting credit information from various interested parties.

Camera surveillance in public transport means
The Budapest Transport Company (BKV) initiated a consultation with the Commissioner about the possible installation of cameras on board BKV transport. The Commissioner pointed out that passenger consent cannot be the legal basis for the processing and, this being the case, due to specific points of Hungarian law, the processing may only be lawful if it is provided for by

an act. The legislator shall find an appropriate balance between privacy and public order considerations. The opinion of the Commissioner was supported by the Hungarian National Institute of Criminology and the latter suggested alternative ways of improving security in public transportation.

Ireland

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

Both Directives have been fully transposed into Irish law.

Legislative developments having a significant bearing on data protection in Ireland during 2009 included publication in July of the Communications (Retention of Data) Bill 2009 giving effect to Directive 2006/24/EC on the retention of data processed in connection with the provision of publicly available electronic communications services (amending Directive 2002/58/EC).

B. Major case Law

In most cases, in accordance with Section 10 of the Irish Data Protection Acts 1988 and 2003, complaints submitted to the Commissioner are resolved amicably without resort to a formal decision or enforcement action. Such amicable resolutions may, for example, involve a financial contribution by the relevant data controller to the data subject concerned or to an appropriate charity. Where necessary, enforcement powers are used – for example, when data controllers fail to respect the access rights of data subjects. In some cases, data controllers are named in case studies included in the Commissioner's Annual Report. In the course of 2009, the Commissioner engaged in several successful prosecutions related to the rights of data subjects under the Data Protection Acts 1988 and 2003 and under Statutory Instrument 535 of 2003 (implementing Directive 2002/58/EC in Ireland). This followed a number of snap inspections of companies engaged in the mobile text marketing sector in 2007 and the successful defence of a High Court challenge to the legal basis for the prosecutions in 2008.

C. Major specific issues

Also in 2009 the Irish Minister for Justice, Equality and Law Reform established a Data Protection Review Group to make recommendations on whether Irish Data Protection legislation needs to be amended to provide for mandatory notification of data breaches with penalties. To date the Group has published a consultation document, issued a public request for submissions, launched a consultation exercise among group members and undertaken extensive desk research.

Italy

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

The regulatory framework on the implementation of directives 95/46/EC, 2002/58/EC and 2006/24/EC did not undergo any major changes in 2009. However, Parliament enacted a few measures that led the DPA to voice its concerns as regards their possible negative impact on the protection of personal data.

More specifically, Act no. 15/2009 on the enhancement of productivity in the public sector introduced an amendment to Section 1 of the DP Code (196/2003) whereby *"The information on performance of the tasks applying to any entity in charge of public functions including the respective evaluation data shall not be the subject of privacy safeguards."* The DPA drew the Government's attention to the advisability of moving this provision to the chapter in the DP Code that regulates the processing of operations by public bodies and also questioned its conformity with both Constitutional and Community law – as certain items of information and whole categories of data subjects are placed outside the scope of protection afforded by data protection legislation.

Section 130 and Section 162 of the DP Code were also amended in 2009 to enable the companies that had created databases by extracting information contained in public telephone directories prior to 1 August 2005 to continue using such data for promotional purposes; a public opt-out register was also introduced and placed under the DPA's supervision. It should be recalled that on 28 January 2010 the European Commission sent the Italian Government a letter with a request for information on the above amendments, as it found that the latter were in breach of directives 2002/58 and 95/46 – this being the first step in the infringement procedure established by Community law.

On a different note, reference should also be made here to Act no. 69/2009, which introduced various requirements to foster the computerisation of public administrative agencies and the online publication of judicial decisions. Relevant data protection provisions are contained in section 21 thereof, which requires public administrative bodies to publish senior officials'/executives' annual salaries, CVs, e-mail addresses and office phone numbers on the respective websites; section 32, whereby the requirements applicable to the publication of administrative decisions and instruments are fulfilled by publication of such decisions and instruments on the relevant agencies' websites; section 36, which is aimed at expediting the implementation of the "public connectivity system" to ensure "full interoperability of databases and census registers" in order to afford better services to citizens and enhance the efficiency of the public administration; and section 45, which amends the civil procedure code by allowing judicial decisions to also be published on Internet websites.

Another important piece of legislation enacted in 2009 aimed at implementing the provisions contained in the Prüm Treaty by setting up the national DNA database and laying down the relevant procedural mechanisms (Act no. 85/2009). The national DNA database will be set up at the Ministry for Home Affairs and include DNA profiles obtained in the course of judicial proceedings along with those of missing persons and/or their blood relatives, unidentified corpses and human remains, and individuals placed under judicial measures restricting their personal freedom. The Italian DPA will be in charge of supervising this database. Most of the suggestions and amendments proposed by the DPA were taken on board, in particular those aimed at ensuring respect for individuals' dignity and proportionality of processing operations; additional safeguards will have to be set forth via secondary legislation, to be adopted after consultation and/or in agreement with the Italian DPA. However, the recommendations concerning the overly broad scope of the provisions on obtaining DNA samples by coercive means and the excessively long data retention periods were not dealt with satisfactorily.

Written Submissions to Parliament – A written submission to Parliament was made in December 2009 concerning advisability of passing ad-hoc legislation to regulate *whistleblowing* (integrity lines) in the corporate sector. The DPA drew attention in particular to the need to regulate the lawful use of personal data collected via the "good faith" reports lodged by whistleblowers as well as access by data subjects to their own data collected in this manner.

Parliamentary Hearings – The DPA was heard several times in 2009 on major issues addressed by the relevant parliamentary committees, either within the framework of fact-finding initiatives or in the course of the debate leading to the adoption of bills that impacted on personal data protection. Reference should be made in particular to the hearing of 30 January 2009 before the Parliamentary Committee for Security of the Republic on a case involving the collection of personal data in the course of judicial investigations and the role of court-appointed experts and consultants; the hearing of 15 July 2009 before the Constitutional Affairs Committee of the Chamber of Deputies, which was part of a fact-finding initiative on computerisation of public administrative agencies; and the hearing of 25 November 2009 before the Financial Committee of the Chamber of Deputies, which was part of a fact-finding initiative on consumer credit with particular regard to credit reference agencies, implementation of the relevant code of conduct and professional practice, and the bills related to identity thefts and fraud in this area.

B. Major case law

Telephone Wiretapping

The **Council of State** (last instance of the court for administrative proceedings) ruled that a civil servant could be lawfully dismissed from office if the relevant disciplinary proceedings relied on tapping transcripts included in the case file of the criminal proceeding that had been instituted against said civil servant on the same grounds and had resulted in his acquittal – even though the transcripts in question had been found to be inadmissible in the criminal proceeding for having been acquired in breach of the law. The facts underlying the disciplinary proceedings were not questioned. Accordingly the issue as to admissibility of the transcripts had to be considered irrelevant (decision no. 7703/2009).

The **Constitutional Court** ruled that destruction of files including unlawfully acquired tapping transcripts should always comply with the rules on the right to be heard, so as to reconcile privacy requirements with due process (decision no. 173/2009).

The **Court of Cassation** addressed the same issue by ruling that the destruction of tapping transcripts should be ordered, in all stages and before all instances of judicial proceedings, by the court that declared them to be inadmissible (where a dispute had arisen as to their admissibility); however, destruction should only take place once said judicial decision becomes final (decision no. 25590/2009).

Medical Data

HIV tests, informed consent, data dissemination

The **Court of Cassation** (civil law division) ruled that as a precondition for administering HIV tests, the patient had to be informed and allowed to give his/her consent thereto, if the patient was capable of making a free, informed decision. This requirement can only be waived if the medical treatment proves objectively urgent and/or specifically necessary in the public interest. The medical staff must take all the necessary measures to ensure confidentiality and prevent dissemination of the information on outcome of the test and/or on the patient's health. In the case at issue, dissemination of this information had resulted in the patient's business being shut down, whilst the patient would have undergone the test in another hospital if he had been informed appropriately (decision no. 2468/2009).

Miscellaneous Issues

Disclosing information on the members of a professional association. The **Council of State** upheld the decision whereby the board of a professional association had only disclosed the personal information the association was entitled to hold pursuant to a specific law. The association had actually withheld the additional personal information requested by the applicant – i.e. address of the professionals' firms, telephone and fax numbers, and e-mail addresses – because such additional information had been communicated to the association on a strictly confidential basis (decision no. 7946/2009).

Image as "personal data". The **Court of Cassation** ruled that an individual's image, though capable of identifying that individual, was not automatically "personal data" under the terms of the DP Code; to that end, it should be expressly related to the individual by way of a caption or any other means (e.g. a verbal statement) enabling identification of that individual. If this is not the case, the image is irrelevant as personal data (decision no. 12997/2009).

Documents containing personal data. According to the **Court of Cassation**, the production of documents containing personal data in judicial proceedings is permitted without the data subject's consent if this is necessary to exercise one's right of defence, irrespective of how the personal data was acquired; this stance by the Court is in line with a previous decision by the DPA. However, the right of defence exercised by relying on another's personal data should not be to the detriment of the requirements of fairness, data relevance and non-excessiveness set forth in the DP Code (decision no. 3358/2009).

C. Major specific issues

Raising Youth Awareness and Social Networks
The Italian DPA decided to launch an initiative targeting students on the occasion of European Privacy Day (28 January). The initiative was called "Cinema & Privacy" and lasted four days; it was aimed at raising youth awareness of the importance of protecting privacy in today's society and of the need to learn how to protect one's privacy. Movies chosen as particularly relevant in addressing privacy issues from different standpoints were shown in the conference room of the Italian DPA. Each movie was introduced by one of the four members of the DPA's collegiate panel as well as by a video specially created by the Italian DPA to describe – again with the help of movies – minor and major intrusions into our private sphere. Students from high schools in Rome were invited to the shows and called upon to discuss and exchange views.

In addition, a booklet was produced by the DPA in 2009 to provide guidance (especially to youths) in dealing with social networks and making knowledgeable use of their potential. The booklet, called "Social Networks: Watch out for Side Effects" was made available free of charge in the main Italian post offices. This initiative was aimed at helping both experienced and inexperienced users to take full advantage of the potential inherent in these innovative communication tools without endangering their private and professional lives.

Database Security
The DPA reviewed and recast (on 25 June 2009) a decision dated 28 November 2008 to enhance the safeguards for data subjects in connection with the activities performed by "system administrators" – a concept that is actually not expressly defined by Italian law. The new text was intended to clarify various points, partly to take into account queries lodged with the DPA. The requirements set forth by the DPA had to do more specifically with access logging (systems must be in place to log access to processing systems and electronic databases performed by system administrators, e.g. via timestamps and event descriptions, without recording the activities performed by system administrators following their access); supervision by data controllers on the activities performed by system administrators (to verify that they are complying with the organisational, technical and security measures provided for in data protection legislation); drafting of a list of system administrators and their features (containing information identifying the system administrators including a list of the functions assigned to them), which should be reported by each data controller in an internal document that should be made available for inspection by the DPA. The DPA highlighted the need to take special care in assessing experience, skills, and reliability of any individual that is entrusted with system administrator functions, particularly to ensure full compliance with data protection legislation and security.

Sensitive Data and Health Care
Online Examination Records. The Italian DPA provided guidance on the use of personal data in connection with "online access to examination records". The Guidelines are meant to lay down a specific, unified framework for safeguarding citizens, particularly in relation to the optional nature of online access to examination records. Data subjects should be allowed to freely decide whether or not to access the online examination records service based on a specific information notice and after obtaining ad-hoc consent for the processing of personal data related to the service in question; they should in all cases continue to be allowed to obtain such examination records on paper at the individual health care provider(s). Specific technical arrangements are set forth to ensure appropriate security measures: secure communication protocols based on encryption standards for electronic data transfers, including digital certification of the systems delivering network-based services; suitable arrangements to prevent acquisition of the information

contained in the electronic file if the latter is stored in local and/or centralised caching systems after being consulted online; and short-term (maximum 45-day) availability of the online examination record.

Guidelines on the Electronic Health Record and the Health File. The Guidelines suggest that the Electronic Health Record should be set up by prioritising solutions that do not entail duplication of the medical information created by the healthcare professionals/bodies that have treated the given data subject.

Since the medical data and documents contained in an EHR are collected from different sources, appropriate measures should be taken to make it possible to trace the entities responsible for creating and collecting the data and make them available via the EHR (also with a view to accountability). In particular, in light of the fact that separate clinical records are at issue, it should be ensured that each entity that has created/drafted those records continues to be, as a rule, the sole data controller of said records.

The data subject must be in a position to freely decide whether or not an EHR/HF should be set up by including the medical information concerning him; his consent must be given on a separate, specific basis; suitable explanations should be provided to data subjects. Partial consent limited to a certain scope should be envisaged to enable data subjects to indicate their wishes. Specific limitations are laid down on the purposes served by the EHR/HF, by clarifying that processing personal data via an EHR/HF must only be aimed at prevention, diagnosis and treatment activities in respect of the data subject; accordingly, it should only be performed by healthcare practitioners. This modular approach makes it possible, for instance, to select the healthcare information that can be accessed by the individual data controller authorised to access the EHR as a function of the respective sector of practice - e.g. an oncology network made up of operational units specialising in cancer treatment. Similarly, some categories of practitioner such as pharmacists may only access data (or data modules) that is indispensable to administer drugs.

Public Transparency and Online Posting of Medical Data. The DPA ordered that medical information relating to over 4,500 disabled individuals be taken off a Regional institutional website and also initiated sanction proceedings against the relevant local authority. It was found that the list of disabled individuals that had been granted an allowance by the Region to purchase a PC could be browsed freely online – including their names, disabilities, places of residence and birth dates. The DPA confirmed that medical information may not be disseminated without any safeguards and that public transparency requirements should not override data protection obligations as applicable to public bodies – in particular, the obligation not to disclose excessive information in relation to the specific purposes.

National and Regional Registries of Mammary Prostheses. The DPA objected to the compiling of a registry including the names of women that have had mammal prostheses implanted, in connection with a governmental bill related to breast surgery. It was recalled that the plastic surgery could be monitored while respecting the anonymity of the individuals operated upon and using statistical codes and tools. The DPA pointed out that it was necessary to establish who would be entitled to access the registry and for what specific purposes, since the wording used in the bill was excessively vague.

Businesses

Mergers and Split-ups – The DPA clarified what obligations should be fulfilled by companies in cases of mergers (by absorption and/or amalgamation) and split-ups to ensure compliance with privacy legislation. In particular, the companies involved should notify their customers, employees and suppliers of the name(s) of the new data controller and data processor(s), if any; to that end, simplified mechanisms may be used such as posting the information initially on the companies' websites and providing individual information to their personnel thereafter.

Business Information Services – The DPA exempted various companies providing business information services from the obligation to provide information notices to all data subjects, as it found that this obligation entailed a disproportionate effort compared to the interests at

issue; however, the DPA required effective alternative measures to be deployed by the companies involved.

Anti-Money Laundering Legislation and Financial Brokers – It was clarified that financial brokers belonging to the same corporate group may lawfully communicate and process personal data without the data subjects' consent in connection with reporting "suspicious" transactions as long as this reporting activity is in line with anti-money laundering legislation and is aimed exclusively at countering money laundering.

Company Registers – The DPA clarified that the DP Code does not place any limitations on access by shareholders to the personal data contained in company registers, nor is it in conflict with the openness of corporate activities. Shareholders are entitled to know addresses and personal information related to other shareholders in order to contact them and defend their legitimate claims.

Telephone and Electronic Communications

Telemarketing. The possibility to re-use (until 31 December 2009) the data contained in telephone directories set up prior to 1 August 2005 for marketing purposes without the data subjects' consent, introduced by Act 14/2009 (see 12th Annual Report), had prompted the Garante to clarify the limitations applying to compilation and use of such data via an ad-hoc decision (March 2009). More specifically, the DPA had required, inter alia, that the data controllers wishing to use this provision to provide proof that the data had actually been extracted from telephone directories compiled prior to 1 August 2005 and to only use the data to contact subscribers for promotional purposes, i.e. it was clarified that marketing companies were prohibited from contacting subscribers in this manner to surreptitiously obtain their consent to use their data for promotional activities after 31 December 2009. Following the amendments made to the DP Code by Act 166/2009 (see above "Legislative Developments"), which extended the deadline for using the data in question and also provided for the establishment of an "opt-out register" applying to telemarketing by 25 May 2010, the DPA decided to extend enforceability of the requirements laid down in the above decision accordingly. On this same note, the DPA rejected the practice of using randomly created phone numbers to contact subscribers for promotional purposes, as it found that such numbers, though created via randomised mechanisms, do represent personal data under the Italian DP law and as such enjoy all the safeguards provided for in the law – including the need to obtain the subscribers' informed consent prior to using them.

Customer Profiling. Specific obligations were imposed by the DPA (decision dated 25 June 2009) on the providers of publicly available electronic communications services as regards profiling of their customers. A detailed analysis was carried out which led to a distinction of different categories of profiling, requiring data controllers to make different arrangements. In particular, two scenarios were envisaged: 1. profiling based on "identifiable" personal information, which requires the data subjects' free, informed, and specific consent; 2. profiling based on "aggregate" personal information, i.e. aggregate data derived from identifiable personal information, which requires either the data subject's consent or, where this has not been obtained, a prior checking application to be lodged with the DPA by the data controller pursuant to Section 17 of the DP Code. In the latter case, the level of aggregation (i.e. the level of detail of the aggregated data) and the technical arrangements applicable to the processing will have to be taken into account. Additional obligations such as notification to the DPA and the provision of appropriate information to data subjects were also laid down.

Journalism

On several occasions, the DPA had to step in to safeguard privacy rights of children. In particular, a few newspapers were prohibited from publishing names and pictures of children involved in reported cases and/or from providing information that would make it possible to identify those children. In child abuse cases, the DPA recalled that it was necessary to safeguard the privacy both of the children and of the other individuals involved by refraining from disclosing the child's age, sex and place of residence; the relationship between child and suspect, if any; or the father's job or profession.

Several requests were lodged with the DPA to have data and pictures available on the Internet (e.g. via Google, Emule, YouTube, forums, and blogs) erased. In some cases the DPA could not take any steps directly because the controller of the Internet website was not resident

in Italy; conversely, in other cases instructions were provided to the data controller to erase the pictures/data considered to be in breach of the law.

Two cases handled by the DPA concerned newspapers and TV channels that had published pictures taken directly from Facebook when commenting on the death of two individuals, even though the pictures in question did not correspond to the deceased individuals, but rather to namesakes. The DPA found that publication of those pictures was in breach of data protection legislation as accuracy of the information collected had not been checked thoroughly and erroneous personal information had been disseminated. It should be pointed out that an increasing number of complaints relate to the processing of personal data extracted from Facebook profiles; misuse of personal information and defamation are the most frequent complaints in this regard.

Another important decision in this area reiterated that filming and using images of individuals within private premises without the individuals' consent was unlawful. The DPA prohibited the dissemination/publication, by any party, of images acquired and/or obtained in breach of the safeguards applicable to private premises, particularly considering the privacy-intrusive techniques implemented to capture those images, the lack of consent by the relevant data subjects, and the exclusively personal nature of the activities shown in those images.

Formal Complaints

In 2009, 360 decisions were made in relation to formal complaints (which are specifically regulated). As in previous years, most of them related to banks, financial companies and credit reference agencies. However, the most interesting issues were to do with the voice as personal data, the exercise of data protection rights concerning deceased persons, and the posting of publicly available information on the Internet.

Voice as personal data. The DPA granted the complaint lodged by a consumer against a telephone operator that had implemented a contract based on a "verbal order". The DPA found that the recording of the call should be made available to the data subject requesting it, as it was not enough for a summary transcript of the relevant contents to be provided. The rights set forth in data protection legislation can be exercised by data subjects also in respect of sound and image data, which is personal data; accordingly, the right to access the personal data contained in the "verbal order" is only fulfilled by making the recording of the call available so that the specific voice data can be accessed.

Clinical records of a deceased person. The DPA granted the complaint lodged against a university hospital that had failed to reply to several requests for personal information related to the treatments that the complainant's partner had undergone. The DPA found that the partner of a deceased person had the right to access that person's clinical record in order to establish judicial claims on the conduct of the care providers. Under section 9(3) of the DP code, the right to access personal data related to deceased persons "may be exercised by any entity that is interested therein or else acts to protect a data subject or for family-related reasons deserving protection" – and the complainant had clarified that the data in question was necessary with a view to taking legal action to establish the care providers' flawed and/or negligent conduct.

Online publication of the resolutions by a municipal body. The DPA ordered a municipality to erase the complainant's address from a resolution that had been posted on the municipality's institutional website and could be retrieved by means of external search engines. The complainant had claimed that blanking his address from the resolution was not in conflict with the transparency of electronically published public instruments and records. The DPA pointed out the need to carefully select the personal data to be published in this manner, as their publication must be proved as necessary under the specific circumstances for the purposes sought by the given measure in accordance with the principles of relevance and non-excessiveness and by balancing the right to privacy with the obligation to ensure publicity of the decisions made by a local authority. Publishing the resolution at issue in full disproportionately impacted the complainant's rights as it led to the dissemination of irrelevant information on the web.

Inspections

The DPA was also strongly committed to inspection activities in 2009. Based on six-monthly inspection plans,

a total of 449 inspections were carried out. In performing such inspections, the DPA can make use of a specialised corps within the Financial Police, which is in charge of checking compliance with the requirements concerning notification, information notices, security measures, and enforcement of the resolutions adopted by the Garante. Forty-five inspections were carried out directly by the inspection department at the DPA concerning, in particular, public bodies that access the information system of the Revenue Service (13); companies providing databases to third parties for marketing purposes (10); and telephone operators in relation to the retention of traffic data for customer profiling purposes (9). As for the inspections performed by the Financial Police on the DPA's instructions (which specify data controller and scope of the inspection), the following areas were covered: private hospitals (35); public hospitals and nursing homes (35); public transport companies (30); recruitment companies (26); suppliers of building materials (25); golf clubs (25); businesses controlled by municipalities dealing in waste collection (20); sales of methane (20); sales of water (20); tourist resorts (20); betting agencies (15); ski lift companies (10); companies selling electronic wares (10); pharmacies (20); companies that registered the use of databases on credit worthiness/defaults (20); other entities as per the specific requests made by legal departments at the DPA (83).

Following the inspections, 43 reports were referred to judicial authorities and 368 procedures initiated to issue administrative sanctions; in addition, in about 150 cases, proposals were submitted to the relevant legal departments at the DPA to impose obligations on the data controllers aimed at bringing processing operations in line with the law.

170 sanction procedures were finalised in 2009 and a total of 1,572,432 euros were levied in fines.

As for criminal cases, several were related to a failure to take minimum level security measures (24). In addition, unlawful data processing operations (7), the provision of false statements and information to the DPA (6), and non-compliance with orders/measures issued by the DPA (4) were detected.

Latvia

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

Personal Data Protection Act

Directive 95/46/EC was transposed into national law by the Personal Data Protection Act that came into force on 20 April 2000. The latest amendments came into force on 1 July 2009. The Personal Data Protection Act was amended on 12 June 2009 and the main changes relate to exceptions in the notification of personal data processing to the State Data Inspectorate and to the obligation to submit a request to the controller in case of possible breach of the Personal Data Protection Act before the complaint is submitted to the State Data Inspectorate. The amendments also establish that the State Data Inspectorate shall no longer accredit internal and external data processing auditors.

Furthermore, the drafts of two additional amendments to the Personal Data Protection Act have been drawn up:

- regarding the exception to enter into the agreement on data transfers to third countries in the field of law enforcement if it concerns international cooperation on national security and in the field of criminal law;
- regarding decisions of the State Data Inspectorate that provide for the interception or interruption of data processing, the amendment provides that the decisions cannot be repealed in the case of an appeal decision.

State Data Inspectorate Act

In order to ensure the complete independence of the Latvian State Data Inspectorate, the process of establishing the draft State Data Inspectorate Act has been completed. Due to the need to review the means required for operation of the independent data protection authority in relation to the economic situation in Latvia, the draft act was updated in 2009. The announcement of the Act is suspended until the European Court of Justice has made a decision on the independence of the German data protection authority.

Regulation on data transfer to third countries

In 2009, the Latvian State Data Inspectorate continued its activities to establish the Regulations of the Cabinet of Ministers on Standard requirements for agreements for personal data transfer to third countries. The regulation implements the requirements regarding content of contracts stipulated in the Commission's Decisions 2001/497/EC and 2004/915/EC on Standard Contractual Clauses for the transfer of personal data. The Regulations will be announced after the amendment in Article 28 Personal Data Protection Act. The amendment has already been drawn up and sent to the Parliament.

Regulation on Requirements for an Audit report on personal data processing in state and local government institutions

The budgetary cut and reduction of functions and administrative capacity of the State Data Inspectorate led to the amendments to the Personal Data Protection Act which came into force on 1 July 2009. These amendments stipulate that accreditation of personal data processing auditors is no longer essential. Instead, it is stated that the requirements for audit reports are determined with the Regulations of the Cabinet of Ministers. In 2009, the State Data Inspectorate drew up the Regulations of the Cabinet of Ministers (17 November 2009 No.1322) "Requirements for an Audit report on personal data processing in state and local government institutions," which came into force on 25 November 2009. The regulation specifies that the content of audit reports on personal data processing in state and local government institutions should be submitted to the State Data Inspectorate once every two years and should contain a risk analysis of personal data processing, an evaluation of compliance with legal acts regarding personal data processing for each separate data processing purpose, the conclusions including risk ratings, and recommendations on improvements.

Freedom of Information Act

Due to amendments to the State Budget Act for 2009 that substantially cut the budget of the State Data Inspectorate, the State Data Inspectorate drew up an amendment to the Freedom of Information Act establishing that the supervision of the Freedom of Information Act has not been within the competence of the State Data Inspectorate since 1 July 2010.

Information Society Services Act
Due to amendments to the State Budget Act for 2009 and the cut to the State Data Inspectorate's budget, the State Data Inspectorate has drawn up an amendment to the Information Society Services Act. The amendments establish that the State Data Inspectorate is obliged to start an investigation when a person has received 10 commercial communications from one sender within a period of one year; however it does not exclude the self-initiative investigations of the DSI.

Regulations on data retention of Electronic Communication Services for law enforcement purposes
Directive 2002/58/EC and Directive 2006/24/EC are transposed into national legislation by the Electronic Communications Act.

From 2007, the State Data Inspectorate has been the responsible authority for summarising the statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network that has been processed by electronic communication service providers in accordance with Article 19 of the Electronic Communications Act and Article 10 of the Directive 2006/24/EC *on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks amending Directive 2002/58/EC*. The Regulations of the Cabinet of Ministers of Latvia (4 December 2007, No.820) "Order on information requests from pre-trial investigation institutions, subjects of investigation actions, state security institutions, prosecutors and courts and on the provision of data retained by the electronic communication service providers, as well as the order on how to summarise the statistical information on the requested retained data and how to submit it" specify the timeframe for how long the electronic communication service providers are obligated to store the data and submit the statistical data to the State Data Inspectorate. In 2008, for the first time the Latvian State Data Inspectorate summarised the statistics.

In accordance with Article 4 of the Electronic Communications Act, protection of personal data in the electronic communications sector shall be supervised by the State Data Inspectorate. In 2009, the State Data Inspectorate faced a problem regarding different interpretation of legislation on the rights of the State Data Inspectorate to access retained data. Since it was necessary to resolve the problem, the State Data Inspectorate drew up an amendment to the Electronic Communications Act and it is expected that the amendment will come into force in 2010.

B. Major case law

The State Data Inspectorate received 140 complaints in 2009, mostly relating to the processing of personal data without legal grounds and data processing that is excessive in relation to the purpose of data processing (in 20 cases the complainant received instructions from the State Data Inspectorate on how to solve the data protection breach by dealing with the controller directly). As a result of inspections carried out by the State Data Inspectorate, violations of the Personal Data Protection Act were confirmed in 58 cases. Regarding the violations detected, warnings were issued in 29 cases, in other words, for 50% of the reported administrative violations. This is an increase on the percentage of previous years. In 2008, warnings were issued in 18% of cases, and in 2007 – in 10% of cases. An additional 18 cases were initiated by the State Data Inspectorate. The total amount of the fines imposed by the State Data Inspectorate amounted to 23,800 lats (about 34,000 euros). Most complaints related to data processing without legal grounds, violation of the data subject's rights (Article 10 and 11 of Directive 95/46/EC) and violation of the proportionality principle in data processing.

The most common violations of personal data processing related to:
- publishing personal data on the internet;
- data processing by credit reference agencies and data transfer to third persons;
- use of personal data by another person for identification purposes in cases of administrative breaches;
- video surveillance;
- data processing carried out by house maintenance services.

The specific case that drew the attention of the media was video surveillance which covered the fitting room areas in a large supermarket chain. In 2009, the number of cases of people using somebody else's personal data when the police checked identities increased.

C. Major specific issues

At the national level, the State Data Inspectorate participated in discussions related to several topics, for example:

- amendments to legal acts related to budget cuts (including the reduction of the functions and administrative capacity of the State Data Inspectorate);
- data processing in state level systems for educational purposes;
- the use of body scanners in prisons;
- publication of court decisions and data anonymisation;
- data processing regarding consumer credit and debt collection; and
- access to databases during vehicle insurance purchases (online purchasing systems).

Specific cases (relating to the most common reasons for complaints):

1. A significant part of the complaints received related to the publication of personal data on the internet without the consent of the data subject. The decisions of the State Data Inspectorate were made on violations regarding data processing without legal grounds.
2. A large part of the complaints related to credit references and the transfers of personal data of debtors to third persons with the aim of collecting debts. Violations are related to the lack of the data subjects' consent for such data transfers. In most cases, the transfers of personal data to third persons is considered as data processing without legal grounds and exceeds the purpose of data processing.
3. Video surveillance without legal grounds or extensive data processing regarding video surveillance. In such cases, video surveillance is, in most cases, considered as excessive personal data processing or as data processing without legal grounds and exceeds the purpose of data processing.

The representatives of the State Data Inspectorate participated in 7 workshops with lectures regarding data protection and spam and direct marketing issues. The target groups were merchants, administrative personnel of city councils and several large companies, teachers and social workers of schools, students and pupils.

Data Protection Officers

In 2009, the Latvian State Data Inspectorate organised four examinations of Data Protection Officers and certificates were issued to seventeen data protection officers who represent both the private and governmental sectors. The training of Data Protection Officers in 2009 is carried out by the private sector.

Drafted recommendations and guidelines

In 2009, the State Data Inspectorate drew up the "Recommendation on Data Transfer to Third countries". In light of the number of questions received by the State Data Inspectorate regarding clarification of Article 28 of the Personal Data Protection Act regulating personal data transfer to third countries, the State Data Inspectorate issued a recommendation on this matter.

With the view to clarifying the personal data processing notification process at the State Data Inspectorate, guidelines for controllers were drawn up, especially taking into account the recent amendments to the Personal Data Protection Act regarding notification exceptions.

Data Protection Day 2009

During Data Protection Day 2009, the State Data Inspectorate carried out activities on personal data protection regarding photography and personal data processing carried out by photographers (amateurs and professionals). A discussion was held between the Latvian associations of photographers, and a representative from the State Data Inspectorate participated in a seminar for photographers where a lecture/workshop regarding photographers' legal liability had been held. One of the issues discussed was how to ensure privacy in photographers' daily work. The State Data Inspectorate presented guidelines to the photographers on personal data protection.

Lithuania

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

- The Act Amending the Legal Protection of Personal Data Act entered into force on 1 January 2009.

  The new wording specifies the provisions for the Legal Protection of Personal Data Act regulating the processing of personal identification codes. According to the new wording, data controllers which process personal data relating to health by automatic means for the purpose of the protection of health and which process personal data for the purpose of scientific medical research purposes must notify the State Data Protection Inspectorate and apply for prior checking. In addition, the term "video surveillance" has been defined, and regulations were adopted regarding the processing of personal image data, the processing of personal data for direct marketing and solvency evaluation purposes. Furthermore, regulations were adopted regarding the status of a person or of a unit responsible for data protection and the complaints handling procedure. The new wording of the Legal Protection of Personal Data Act establishes the independence of the State Data Protection Inspectorate functioning as a supervisory institution for data protection with a 5-year term of office for the Head of the Inspectorate.

  Though the new version of the Legal Protection of Personal Data Act entered into force only on the 1 January 2009, a new Draft Law Amending the Legal Protection of Personal Data Act is currently under preparation. This draft covers amendments on legal status/independency of the State Data Protection Inspectorate and on processing of personal data for solvency evaluation purposes.

- The amendments to the Electronic Communications Act transposing Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or Public Communications Networks and Amending Directive 2002/58/EC entered into force on 16 March 2009.

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

  If this data above is needed by entities engaged in operational activities, institutions involved in pre-trial investigations, courts or judges in order to prevent, investigate and detect criminal acts, the institutions authorised by the Government - on the instruction of the entities engaged in operational activities - the entities providing electronic communications networks and/or services must store such information for a longer period, but no longer than an additional six months. Such storage shall be paid for by state funds in accordance with the procedure established by the Government (Article 77(2) of the Electronic Communications Act of the Republic of Lithuania).

  The State Data Protection Inspectorate is responsible for supervising the implementation of the provisions of Chapter 9 of the Electronic Communications Act, which also covers the provisions transposing Directive 2006/24/EC.

- A Government Resolution amending the Government Resolution "On Granting Authorisation for implementing the Electronic Communications Act" No. 788 was adopted on 22 July 2009. The State Data Protection Inspectorate was designated as the institution responsible for collecting and providing the European Commission with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network according to Article 10 of Directive 2006/24/EC.

- The Government Resolution "On the Approval of Procedures for Providing Statistical Data foreseen in the Article 70 of the Electronic Communications Act" No.789 was adopted on 22 July 2009. This resolution describes the procedures setting out how law enforcement institutions must provide the traffic data stated in Article 10 of the Directive 2006/24/EC to the State Data Protection Inspectorate and how the State Data Protection Inspectorate must forward it to the European Commission.

B. Major case law

Definition of personal data

The State Data Protection Inspectorate issued an administrative offence record for a company that had collected personal data (full names and addresses) from another company and used it to send offers to these people to change contractor. The State Data Protection Inspectorate decided that there were no lawful grounds for processing the personal data.

The Kaunas district court stated that the definition of personal data provided in paragraph 1, Article 2 of the Legal Protection of Personal Data Act does not cover first name, surname and address of natural persons and, therefore, the Legal Protection of Personal Data Act does not regulate legal protection of such data.

An appeal was lodged with the Supreme Administrative Court of Lithuania against the decision of the Kaunas district court. The Supreme Administrative Court stated that according to paragraph 1, Article 2 of the Legal Protection of Personal Data Act, personal data shall mean any information relating to a natural person or the data subject who is or can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In addition, a parallel definition is provided in paragraph a, Article 2 of Directive 95/46/EC. Considering these definitions, first name, surname and address should be considered as personal data because a person can be identified by means of such data. The Supreme Administrative Court also noted that the European Court of Justice considers such data as personal data (Decision of 6 November 2003, case number C-101/2001).

Rights of data subjects

The State Data Protection Inspectorate received a complaint concerning the collection of a complainant's personal data from the Real Property Register. The State Data Protection Inspectorate decided that the criterion for lawful processing of personal data was subparagraph 6, paragraph 1, Article 5 of the Legal Protection of Personal Data Act (personal data may be processed if such processing is necessary for the purpose of legitimate interests pursued by the data controller or by a third party to whom the personal data is disclosed, unless such interests are overridden by the interests of the data subject). Although the data controller (a bank) was obliged to provide the complainant with the conditions relating to the data subjects' rights, this was not done, i.e. the data controller did not inform the complainant of his right to access his personal data on the Real Property Register and did not inform the controller of his right to object to the processing of his personal data. Therefore, the State Data Protection Inspectorate instructed the data controller to ensure that subparagraphs 2 and 3, paragraph 2, Article 18 (the right to know (be informed) about the processing of his personal data) and paragraph 1, Article 21 (the right to object against the processing of his personal data) of the Legal Protection of Personal Data Act (version in force up to 31 December 2008) would be implemented in the future.

The data controller appealed against the instruction of the State Data Protection Inspectorate in court on the basis of the exception provided in subparagraph 5, paragraph 2, Article 17 of the Legal Protection of Personal

Data Act (whereby the data controller must provide the data subject with the conditions for exercising the rights laid down in this Article, with the exception of cases laid down in laws when it is necessary to ensure protection of the rights and freedoms of the data subject or other persons).

Vilnius District Administrative Court stated that the State Data Protection Inspectorate's position that personal data processing is legal, while stating that subparagraphs 2 and 3, paragraph 2, Article 18 of the Legal Protection of Personal Data Act (version in force until 31 December 2008) were breached is illogical. The State Data Protection Inspectorate's acknowledgement that the data controller had legitimate interests in processing personal data and that these interests were not overridden by the interests of the data subject does not take into account the data controller's obligation to inform the data subject that his personal data is being processed. According to subparagraph 5, paragraph 2, Article 17 of the Legal Protection of Personal Data Act, the data controller must provide the data subject with the conditions relating to the rights of the latter laid down in this Article, **with the exception of the cases** laid down in laws when it is necessary to ensure protection of the rights and freedoms of the data subject or other persons. The Vilnius District Administrative Court concluded that the determined factual circumstances justify the legitimate interest of the data controller and comply with subparagraph 5, paragraph 2, Article 17 of the Legal Protection of Personal Data Act, and, therefore, the instruction of the State Data Protection Inspectorate was revoked.

An appeal was lodged with the Supreme Administrative Court of Lithuania against the decision of the Vilnius District Administrative Court. The Supreme Administrative Court agreed with the argument of the State Data Protection Inspectorate that a decision that personal data is processed according to Article 5 of the Legal Protection of Personal Data Act (criterion for lawful processing of personal data) does not presume that personal data processing was done according to all procedures provided in this act. As such, there were no legal grounds for the decision of the court of first instance to state that there was no breach of the provisions regulating the rights of data subjects because the State Data Protection Inspectorate had decided that the criterion for lawful processing of personal data had been fulfilled.

According to subparagraph 5, paragraph 2, Article 17 of the Legal Protection of Personal Data Act, the data controller must provide the data subject with the conditions relating to the rights of the latter laid down in this Article, with the exception of cases **laid down by law** when it is necessary to ensure protection of the rights and freedoms of the data subject or other persons. Therefore, the right of the data controller not to provide the data subject with the conditions for exercising his rights should be accompanied by two conditions: (1) such right of the data controller must be provided for in law, and (2) these actions have to be necessary to ensure protection of the rights and freedoms of the data subject or other persons. In other words, it is not enough for the data controller to want to apply this exception only to try to ensure protection of the rights and freedoms of the appropriate subjects. In addition, such right of the data controller must be provided for by means of a legal instrument. The court of first instance could not state that this exception had to be applied without indicating the other certain legal act because subparagraph 5, paragraph 2, Article 17 of the Legal Protection of Personal Data Act is a directive legal provision.

The Supreme Administrative Court also stated that the data controller did not mention this exception to the State Data Protection Inspectorate when providing all the written explanations in the complaint investigation stage, thus the later arguments on the application of the exception could be considered as an intention to escape responsibility.

C. Major specific issues

Preventive activity

Chapter three of the Legal Protection of Personal Data Act regulates video surveillance. In order to find out the extent to which data subjects' rights are being ensured while processing image data, the State Data Protection Inspectorate carried out inspections at 92 petrol stations.

It was found that 33 out of 92 gas stations do not use video surveillance. Breaches of the Legal Protection of Personal Data Act were discovered in 57 gas stations.

According to Article 31 of the Legal Protection of Personal Data Act, personal data may only be processed by automatic means if the data controller or his representative notifies the State Data Protection Inspectorate. The State Data Protection Inspectorate had only been informed of video surveillance at two of the inspected petrol stations. A further 55 petrol stations processed image data without informing the State Data Protection Inspectorate (11 petrol stations out of these 55 notified the State Data Protection Inspectorate during the performance of the inspections).

It was found that the petrol stations do not properly ensure the right of data subjects' to know (be informed) that their personal data is being processed. 47 petrol stations inform data subjects about video surveillance by special information signs, but do not provide information about the data controller and his requisites as required by paragraph 1, Article 20, of the Legal Protection of Personal Data Act. 27 petrol stations provide information about video surveillance at an inappropriate distance, i. e. data subjects become aware of the video surveillance once they enter the surveillance area.

According to paragraph 3, Article 20 of the Legal Protection of Personal Data Act, if video surveillance is used in the workplace and on the data controller's premises or territories in which the data controller's personnel work, the personnel must be notified of such processing of their image data in writing, according to the procedure laid down in paragraph 1 of the Article 24 of this Law. It was found that just 31 petrol stations had notified their personnel of the image processing in writing.

37 petrol stations do implement the right of data subjects to access their personal data and to be informed of how it is processed, but 15 of them ask data subjects to provide them with a reasoned application even though Article 25 of the Legal Protection of Personal Data Act states that data subjects have the right of access by providing the data controller with their personal identification document and a written application, i.e. without a reasoned application.

According to paragraph 1, Article 18 of the Legal Protection of Personal Data Act, processing of image data must be set down in a written document of the data controller specifying the purpose and extent of the video surveillance, the retention period of video data, conditions of access to processed image data, conditions and procedure of destruction of this data and other requirements concerning the legitimate processing of video data. It was found that 25 petrol stations had no such document. 28 petrol stations did have such documents, but they did not comply with the requirements of paragraph 1, Article 18 of the Legal Protection of Personal Data Act.

The inspected petrol stations were given instructions regarding their breaches of the Legal Protection of Personal Data Act.

Public awareness

European Data Protection Day

European Data Protection Day was celebrated on 28 and 29 January 2009. A meeting with representatives from other state organisations and agencies, involving the resolution of diverse issues relating to the protection of personal data, was organised on 28 January 2009. The representatives of the public sector were informed about the recently inaugurated celebration of the Data Protection Day in Europe, its mission, the topical questions and an overview of the State Data Protection Inspectorate.

An e-conference was organised in the framework of the Human Rights Centre project "Mano teisės" ("My rights"). The answers to questions on the protection of personal data addressed to the Director of the State Data Protection Inspectorate - Algirdas Kunčinas regarding the e-workplace, video surveillance, direct marketing, documents which are disposed of, the competence of the State Data Protection Inspectorate and the rates of penalties imposed for unlawful disclosure of personal data were given on the website.

In addition, the State Data Protection Inspectorate celebrated the European Data Protection Day with a group of librarians on the 29 January 2009. The venue was Vilnius County Adomas Mickevičius Public Library.

The conference dealt with sensitive issues for libraries relating to the protection of personal data, among other things. The event highlighted the most important issues of personal data protection in a wider context to the representatives of the libraries, placing an emphasis on raising awareness in the field of privacy protection. An hour before the start of the conference the lawyers of the SDPI provided legal guidance and consultations on questions pertaining to processing of personal data and privacy protection to library employees and readers.

Various flyers and information brochures, dedicated to the question of the day were published and delivered: "Do You Know Your Rights as a Data Subject?"; "Personal Data Protection and Video Surveillance"; "Personal Data Protection for Users of Wireless Networks".

"Personal Privacy and Data Protection in Lithuania" Conference
The State Data Protection Inspectorate together with a joint stock company "Expozona" organised a conference on "Personal Privacy and Data Protection in Lithuania" on the 26 November 2009. The purpose of this event was to introduce representatives of public and private sectors to privacy and data protection issues in relation to employee privacy, debt collection and video surveillance. Speakers from the State Data Protection Inspectorate participated, as well as speakers from electricity supply companies (UAB "*Eastern Distribution Networks*"), pre-trial debt collection (UAB "Ekskomisarų biuras"), and the Administration of Vilnius City Municipality. Seven presentations were given on the following topics:

- Are we heading towards a "1984" style society? (privacy and publicity in the information society: tendencies and threats);
- An employee has the right to his privacy too;
- Personal data processing: how can it help to develop relations with customers?
- Personal data processing and problems in pre-trial debt collection;
- Legal regulation of video surveillance;
- General requirements for organisational and technical data protection measures;
- Video surveillance system in Vilnius city: now and in the future.

There were also discussions and the members of the conference were able to ask questions and express their opinion on the issues concerned.

The State Data Protection Inspectorate issued *a Recommendation on "Privacy Protection in Video Surveillance Systems. Wireless Communications Technologies"* on 16 December 2009. It gives recommendations on how to protect privacy using CCTV, webcams and other video surveillance means, looks at the risks of using these devices and describes possible organisational and technical data protection measures.

The full text (Lithuanian only) of this recommendation can be found at: http://www.ada.lt/images/cms/File/naujienu/IP%20kamera%20(Galutinis)%2020091216.doc

The State Data Protection Inspectorate issued a *Recommendation on "Safe Data Transfer by https Protocol"* on 23 December 2009. It covers such topics as installation of https protocol, activity principals of https protocol, and types of SSL certificates. The full text (Lithuanian only) of this recommendation can be found at: http://www.ada.lt/images/cms/File/Inspekcijos%20rekomendacijos/SSL20091228.doc.

Luxembourg

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

Law of 2 August 2002 regarding the protection of persons with regard to the processing of personal data (implementation of Directive 95/46/EC)

No amendments to the above-mentioned law were made during 2009.

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

No amendments to the above-mentioned law were made during 2009.

Decrees and secondary legislation
The grand-ducal regulation of 13 February 2009 implementing the "*service cheque*" in the domain of educational day care centres sets out the details of the creation and use of a database relating to such "*service cheques*".

A ministerial regulation dated 10 November 2009 amended the provisions of the grand-ducal regulation of 1 August 2007 authorising the creation and police use of a video surveillance system in public "*security areas*". This ministerial regulation adds a new "*security area*" to the three existing ones, which are areas where permanent video surveillance will be operated by police forces.

The conditions for the delivery of cadastral (land registry) documentation have been detailed in the provisions of the grand-ducal regulation of 9 March 2009.

The government also issued a grand-ducal regulation dated 3 December 2009 setting forth the procedures to be followed in order to establish the death of a person before taking or drawing substances and samples from the deceased person's body.

Other legislative developments
In 2009, the *Commission nationale* advised the Luxembourg government on numerous topics, the most important one being the bill on "*the identification of natural persons, the national register of natural persons and the identity card*", the aforementioned grand-ducal regulation implementing the "*service cheque*" in the domain of educational day care centres, the bill amending the law determining the "*conditions in which magistrates and police officers may have access to certain databases held by public legal entities*", the draft grand-ducal regulation on inter-administrative cooperation and the bill on exchanging certain information pertaining to the tax sector and the signature of bilateral conventions avoiding double taxation.

The Luxembourg DPA also advised the Luxembourgish Association of the Bank and Insurance Employees (ALEBA) on the problem of private transactions carried out by their employees.

B. Major case law

Civil and criminal case law
District Court of Luxembourg, 9th correctional chamber on the validity of proof (video-surveillance images) collected in violation of the 2002 data protection act

The lawyers defending four individuals accused of repeatedly stealing cigarettes and alcohol in service stations all around Luxembourg pleaded "*in limine litis*" that the video tapes used as proof against their clients were to be rejected, as no prior authorisation from the CNPD had been obtained. Hence, they concluded that such proof should be considered null and void and that the criminal proceedings against their clients should be stopped.

The Court, making references to "*private property*" and service station opening times, as well as to a general objective of the act of 2002 (the intent of the act not being the protection of illegal activities), ruled that the tapes may nevertheless be allowed as means of proof. It must be noted that in this case the judges did not invoke a specific provision of the law, but simply made reference to vague judicial concepts deduced from their conviction, which are in direct opposition of previous case law. Such a highly prejudicial interpretation clearly lessens the legal security provided for by the law and one should hope that the appellate judges will use a

proper legal basis of the law to form their opinion on this subject matter.

C. Major specific issues

eBay's Binding Corporate Rules (BCR) approved
The CNPD, acting for the first time as lead authority, formally approved eBay's BCR application for privacy compliance for both customer and employee data.

Following a very constructive and collaborative environment maintained with eBay and the fast liaising (under the mutual recognition procedure) with the data protection authorities of the other 13 EU Member States, the CNPD managed to achieve the approval of the BCR in less than 12 months.

Google Street View
Google Inc. contacted the Luxembourg DPA on the matter of specific national data protection provisions and requirements applicable to their "Google Street View" service, which Google plans to implement in Luxembourg.

The CNPD, following the joint position adopted in February 2009 by various DPAs, decided that the pictures to be taken and published must not conflict with Luxembourg's national data protection legislation, and that Google would have to implement stringent safety measures and specifically ensure that data subjects' rights were observed.

In particular, the right to object to such processing would have to be strictly observed by Google and the procedure to object would have to be kept as simple as possible. The CNPD drafted and published a model letter for all data subjects wishing to exercise their right to object, which would simply be sent by the data subjects to Google Inc.

In May 2009, the CNPD was obliged to suspend the image-taking on Luxembourg territory for the "Google Street View" service, as certain conditions and prerequisites set out by the DPA had not been observed. In particular, Google had not observed the obligation to publish, via the national media or on the Internet, in advance, the exact periods and regions where Google's vehicles would be taking pictures.

After fulfilling all the prerequisites, Google took up the image-taking again in August 2009 in seven municipalities in Luxembourg. The CNPD is currently following all developments relating to this service with increased attention.

Investigation of the main Luxembourg telecommunication companies
During 2009, the CNPD carried out an exhaustive investigation on the "*compliance with the legal requirements concerning the confidentiality and security measures regarding traffic data*" of the main Luxembourg telecommunication companies. This study also covered the questions related to data retention as requested in the context of the common enforcement actions of the DPAs, initiated by the Article 29 Working Party.

Malta

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

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

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

Other legislative developments

None to report for the period under review.

B. Major case Law

None to report for the period under review.

C. Major specific issues

During 2009, the Office received 54 complaints, which prompted the Commissioner to investigate each case in terms of the powers conferred on him by law and communicate the respective decision according to the outcome of the investigations. No decisions were appealed before the Data Protection Appeals Tribunal. The most common subjects of the complaints related to the installation of CCTVs by private individuals and the sending of electronic communications for the purposes of direct marketing without satisfying the requirements established under the Act. During the period under review, the Commissioner carried out numerous inspections on the processing of personal data undertaken by various data controllers; these inspections were carried out in the course of investigating complaints, as part of the Office's strategy to evaluate a particular sector, on the Commissioner's own motion and also to honour European obligations. Data controllers have also submitted requests for prior checking concerning the introduction of biometric systems at the workplace and where processing operations involved particular risks of proper interference with the rights and freedoms of data subjects.

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

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

In line with the Office's strategy to raise data protection awareness, presentations were delivered to various organisations and constituted bodies with the objective to involve the key players in the evolution of the data protection culture. Articles and presentations on

different aspects of data protection were published in local media and presented on the radio and television programmes. Citizens are becoming aware of their rights and this can be quantified by the substantial number of queries, both by telephone and by e-mail, which have reached the Office during such period.

Having regard to the recent Directive of the European Parliament and of the Council amending, *inter alia*, Directive 2002/58/EC, the Office commenced discussions with the Malta Communications Authority to transpose, in the respective national legal instruments, the amendments introduced by the directive. It is being envisaged that in early next year, both authorities will be holding a series of joint meetings with the undertakings with the objective to receiving their feedback on the new and amended provisions. The consultation exercise is deemed to deliver positive results and thus ensuring a smooth transposition process and an effective implementation.

On 28 January, the Data Protection Commissioner joined the other Data Protection authorities in Europe to celebrate the Data Protection Day. To mark this day on the local level, the Office of the Data Protection Commissioner has distributed informative material to students in all state, private and church schools. The uphill task is to get the message across and make citizens, particularly from a young age, aware of the inherent risks which one may be exposed to when providing personal information on the net. It has always been this Office's firm belief that for an effective culture change to happen there needs to be continuous investment in the young generation. Today's children will be our future. Culture takes time to change, but the consolidation of all the elements in the privacy formula will eventually yield the desired results. With the increasing available social networking applications, the privacy boundaries are being blurred and this Office is committed to strengthen the privacy objectives in this regard whilst being guided by the core concept of reasonable expectation to privacy.

In February of this year, Mr Joseph Ebejer was formally appointed to serve in the position of Data Protection Commissioner for a term of five years following the untimely demise of Mr Paul Mifsud Cremona.

Netherlands

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

Directive 95/46/EC was transposed into national law as the *Wet bescherming persoonsgegevens* (Wbp) [Dutch Data Protection Act]. This was achieved by means of the act of 6 July 2000[20] which entered into force on 1 September 2001, replacing the old data protection law, the *Wet persoonsregistraties* (Wpr) dated 28 December 1988.

Directive 2002/58/EC has been transposed into Dutch law mainly by the amended *Telecommunicatiewet* (Telecommunications Act) which entered into force on 19 May 2004[21]. Other legislation transposing parts of this directive are, among others, the *Wet op de Economische Delicten* (Act on Economic Offences) implementing article 13(4) of Directive 2002/58/EC.

B. Major case law

The Dutch Data Protection Act is currently subject to evaluation. In view of the possible revision of the Act, the Dutch DPA [College bescherming persoonsgegevens (CBP)] has stressed the importance of strengthening the position of data subjects. They should have easy access to information about why their personal data is being processed, which measures have been taken to prevent the illegal use of that data, and how they can exercise their rights. Apart from that, easily accessible complaints procedures should be developed/introduced, as well as the possibility of class actions.

As for the position of the controller, a shift is taking place from ex-ante supervision to ex-post supervision. Controllers should invest more in complying with the law and should have to pay for non-compliance. The Dutch DPA encourages more transparency, a requirement to report data breaches and the use of privacy by design. Lastly, the position of the supervisory authority itself should be strengthened by endowing the Dutch DPA with more powers.

In addition to its work as adviser to the government concerning new legislation on privacy, the Dutch DPA, in its supervisory role, opted to give priority to enforcement so that it can make the most effective contribution to the promotion of compliance with the Dutch Data Protection Act. For the purpose of establishing the priorities for 2009, a risk analysis was made of the processing of personal data in different sectors of society. The Dutch DPA subsequently selected cases that contained indications of serious violations of the law, which were structural in nature, affected many citizens, and against which the Dutch DPA had the power to take action. The Dutch DPA also kept its eyes open for topical events in the course of the year. The investigations and interventions carried out by the Dutch DPA (108 in 2009) did not only achieve results with individual controllers, but also appeared to have indirect effects. The thematic 'guidelines' for 2009 entailed the obligation to provide information on and transparency about the transfer of personal data to third parties.

C. Major specific issues

The internet

After an investigation into an internet company, the Dutch DPA concluded that the company had violated the law by collecting sensitive data on people using internet platforms and subsequently selling their profiled personal data to third parties without having informed the persons affected by this clearly and fully. At the time, approximately 2.2 million people were visiting the company's internet sites. The company offered them the possibility to complete a test, for instance, to find out 'your real age'. The investigation revealed that the internet company had collected and processed medical data, among other things, even though this activity is in principle subject to a statutory prohibition. The internet company did not inform the affected people about the use of their data in accordance with statutory requirements.

A site for pupils to assess their teachers caused serious damage to the privacy of the teachers concerned.

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

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

Following an investigation by the Dutch DPA, the site was modified and hidden from search engines.

The Dutch DPA also investigated two sites aimed at young people. The social network site www.zikle.nl was required to inform its users adequately about the purposes for which personal data was collected and processed, to apply security measures and to hide pages containing personal profiles. www.jiggy.nl used a game to entice users to hand over email addresses of other people for direct marketing purposes. After investigation, the owner of the website removed the game.

Financial data

After the introduction of the instrument of an Advisory Letter in 2008, the Dutch DPA drew up its first advisory letter in 2009 at the request of the Stichting Landelijk Informatiesysteem Schulden (LIS), [National Information System of Debts], which was followed by a second advisory letter in response to a new draft of the LIS. Tests conducted by the Dutch DPA revealed that neither of the drafts complied with the statutory requirements. With respect to the second draft, the Dutch DPA concluded that the draft far exceeded the original purpose of the draft, i.e. the registration of overdue debts to avoid problematic debts. This may result in a substantial group of people being registered who do not belong on the register but who will, nevertheless, be subject to the negative consequences of being considered a problematic debtor.

A bank passed on young clients' account numbers and addresses to a charity without informing the clients or asking for their consent. Following a complaint, the Dutch DPA investigated the matter, and as a result, the bank adjusted its practice.

In 2009, the Dutch Finance Minister followed the DPA's advice on legislative proposals for the establishment of a pension register. The idea is that each citizen can check his or her retirement pay rights online. As this data will undoubtedly attract other parties, the Dutch DPA pointed out the need for tight security measures.

Medical data

On the basis of investigations at two current regional electronic patient records systems (reprs), the Dutch DPA established that the Dutch Data Protection Act had been breached. The Dutch DPA initiated compliance procedures against both reprs. These procedures resulted in one of the two reprs ceasing the unlawful activities by, among other things, informing all patients personally about the inclusion of their data in the reprs. Proposed legislation on electronic patient records continued to cause concern. Critical advice from the Dutch DPA on the initial legislative proposal in 2007 led to adaptation of the draft. Amendments by the House of Representatives, however, made it possible in some cases for healthcare insurers to have access to patient records. The Dutch DPA advised the minister to remove this exception to the general prohibition. The Minister has indicated that he will follow this advice.

Another cause for concern relates to information security in hospitals. Investigations carried out by the Dutch DPA and the Inspectie voor de Gezondheidszorg (IGZ) [Netherlands Healthcare Inspectorate] in 2007 and 2008 revealed that none of the twenty hospitals investigated complied with the standard for information security. In 2009, the Dutch DPA imposed orders establishing a penalty for non-compliance on four hospitals that still had not properly organised this aspect.

Investigation into the procedures of a number of occupational health and safety services resulted in the conclusion that at least one service acted systematically in violation of the law by providing medical data of sick employees to their employers even though this data was subject to medical confidentiality. The Dutch DPA imposed an order establishing a penalty for non-compliance on this health and safety service in 2009. The health and safety service subsequently ceased the violations within the compliance period set. The investigation into three other occupational health and safety services has been continued.

Other activities in the private sector

Even though we seem to be getting used to it, camera surveillance is still a widespread phenomenon far-reaching means, in relation to which the Dutch DPA receives a lot of questions from citizens. The Dutch DPA investigated the use of camera surveillance on an industrial estate. The findings were generally positive for the company responsible for the surveillance. The

company promised to change the rules on inspection in order to make them consistent with the requirements of the Dutch Data Protection Act. Since it is not always clear if private companies or government bodies are responsible for camera supervision, the Dutch DPA has decided to develop new guidelines on the subject.

A lot of buzz was generated by the proposed introduction of the so-called 'smart' electricity meter, which can provide a very detailed picture of someone's household and so of the periods in which people are not at home. Consumers should be allowed to make informed choices regarding the frequency and amount of information that can be collected. The draft bill has been amended following the Dutch DPA's advice to the Minister.

Young people

The digital processing of personal data in general, and by the government in particular, demands clear safeguards. This is even more the case for information relating to children and young people. In 2008, the Dutch DPA issued highly critical advice on the draft legislative proposal that would result in the creation of a Verwijsindex Risicojongeren [reference index for young persons at risk]. Criticism focused particularly on the object of the reference index, which is insufficiently concrete and, combined with its unclear criteria for the registration of a young person by his or her care provider, entails an almost inevitable risk of arbitrariness. Although the legislative proposal submitted on 6 February 2009 responded to criticism raised by the Dutch DPA – among others – in several areas, the essence unfortunately remained the same. In 2009, the Dutch DPA was asked for advice on a number of the executory measures that the new bill entails and again, it warned of the risk of arbitrariness.

Primary schools issue educational reports on their pupils to secondary schools. The Dutch DPA has investigated compliance with the obligation to inform children's parents in this situation. This is vital as it provides for the possibility of correcting the report, which can have a protracted negative effect on children if it contains incorrect or outdated information. More than half of the schools that were investigated did not record whether or not parents were informed. Following the investigation, the Dutch DPA issued guidelines for primary schools on the subject.

Police and the judicial authorities

Safeguarding the correct and transparent use of personal data is vital in light of the increased powers that police and the judicial authorities have in relation to the processing of personal data. In 2007/2008, the Dutch DPA investigated the internal exchange of personal data within the police forces via the police information desk. By far the majority of police regions were found to be completely unequipped for compliance with the requirements of the *Wet politiegegevens* [Police Data Act], which became effective on 1 January 2008. In 2009, a follow-up investigation in three regional police forces showed that, though there are some differences in context, none of the forces complied fully with the requirements for authorisation and monitoring.

Intelligence services can compare their information directly with police records. In advice regarding proposed legislation on this independent form of consulting police databases, the Dutch DPA asked the government to clarify why such large-scale consultation was necessary.

In 2009, the Dutch DPA developed guidelines for the purpose of automated number plate recognition (ANPR) by the police. In these guidelines, the Dutch DPA explained its interpretation of the statutory standards as a supervisory authority when exercising its powers. Later the same year, the Dutch DPA conducted investigations into the application of ANPR by two police forces and concluded that both police forces knowingly acted in violation of the Dutch Police Data Act by processing hits and no-hits over 120 or 10 days, respectively. A no-hit means that a scanned number plate does not occur in the reference file and that this number plate is consequently not sought by the police. The registration of this number plate must be destroyed immediately. In response to the publication of the final investigation findings, both forces announced at the beginning of 2010 that they would cease the unlawful practice.

Passengers who want to participate in a system allowing for automated border passage, for example, by means of an iris scan or fingerprints, have to be screened beforehand. The Dutch DPA has asked the Minister of Justice to clarify which starting points will be used in these background investigations.

Poland

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

Revision of the Telecommunications Act
The Act of 24 April 2009 on the amendment of the Telecommunications Act entered into force on 6 July 2009. The amendments were, among others, new provisions on data retention, adapting national legislation to the requirements set forth in the Directive 2006/24/EC by imposing many additional responsibilities on the public telecommunications network operators and providers of publicly available telecommunications services (such as the obligation to retain traffic data for a period of 24 months from the time of the call, and after that time to destroy such data except for data retained under other provisions of law). The above-mentioned obligations should be implemented in a way that does not result in the disclosure of the telecommunication transfer. The introduced amendment also requires that entrepreneurs ensure the security of personal data through appropriate technical and organisational measures and also ensure that this data can only be accessed by authorised staff.

Draft Act on the amendment of the Act on access to public information, which stipulates that data relating to the health condition of the people holding the posts of President and Prime Minister be considered as public information. The Inspector General, clearly expressing his negative attitude towards the provisions of the draft, pointed out that the existing provisions of the Polish Constitution, the Personal Data Protection Act and Directive 95/46/EC all recommend that the legislator maintain far-reaching moderation in terms of introducing provisions that might result in publishing data on so-called health status as "sensitive" - even in the case of holders of the highest public positions in Poland. He stressed that although the right to privacy and the right to the protection of personal data of public office holders is much narrower than that of "ordinary citizens", there is no legal basis that would lead us to assume that these rights should not apply at all. The data protection authority highlighted that this position was also reflected in the Declaration on the freedom of political debate in the media of the Committee of Ministers of the Council of Europe of 12 February 2004.

In light of the firm position of the Inspector General, the above-mentioned draft did not enter into force, and any further attempts to introduce it will meet with a firm response from the DPA.

The new Regulation issued by the Minister of Internal Affairs and Administration on **prototyping a notification of a data filing system to registration** by the Inspector General for Personal Data Protection entered into force on 10 February 2009. In the new specimen notification, drafted at the initiative of GIODO, simplifications were made and the principal responsibilities of the data controller were listed with regard to data safeguarding. The introduction of the new specimen resulted in a decrease in the number of notifications incorrectly filled out.

B. Major case law

During the reporting period, the Inspector General considered several cases relating to the activities of the Credit Information Bureaus. The Supreme Administrative Court agreed with the position of the Inspector General on several cases. One of the most important cases was that the Bureaus, as data controllers, were charging their clients for access to their personal information. This practice has met with strong opposition from the Inspector General. According to Polish provisions, the data subject has a right to access information once every six months and access should be provided free of charge. With reference to the above, such an approach was confirmed in the decision issued by the Supreme Administrative Court on 30 July 2009.

The Inspector General also dealt with the problems of the acquisition and processing of biometric data for the purpose of supervising working time. The Inspector General took the position that such action is an excessive interference in the privacy of the data subject. In such cases there is always a great risk of violation of privacy, and it is necessary to choose other, less intrusive methods. This position was confirmed by the Supreme Administrative Court, which, in its ruling of 1 December 2009 held that in assessing the desirability of obtaining the biometric data of employees, with their consent, for the verification of working time, it should be noted that the major prerequisites for processing in such cases shall be the principles of proportionality and legality. It means that the risk

of breaking freedoms and fundamental rights must be proportional to the purposes for which such data is processed. Since the principle of proportionality expressed in the Personal Data Protection Act is a primary criterion for decisions related to the processing of biometric data, it should be noted that the use of such data to control working time is disproportionate to the intended purpose of their processing. The Court maintained the position that gathering biometric data in such cases would have to be seen as an excessive intrusion into privacy thereby confirming the position of Inspector General.

During the reporting period, the Inspector General also investigated the question of admissibility of processing personal data in the backup copies created by the banks after the removal of data from the data filing system, without having legal grounds for further processing. Such a situation may arise after a rejected credit application, where the bank removes the personal data of the applicant from the filing system as the legal basis drawn from the Data Protection Act has expired (processing of data necessary to undertake activities needed for the conclusion of the contract). In addition, processing data in backup copies, when the data is no longer in the filing system, is contrary to the purpose for which such copies are made (archiving purposes related to ensuring the operational safety of the bank). The above position of the Inspector General was confirmed in the judgment of the Regional Administrative Court in Warsaw of 16 January 2008. The Supreme Administrative Court then dismissed the appeal on 3 July 2009.

C. Major specific issues

In June 2009, GIODO audited the processing of personal data in the IT systems of the Public Transport Authority of Warsaw (ZTM) in light of press articles on how ZTM was recording places and times of public transport travel (particularly in the Warsaw underground, where at each entrance the passengers need to swipe a coded electronic ticket card at the gate in order to open it). The inspection confirmed the existence of the problems identified by the press and other irregularities related to excessive data processing not in line with the purpose. GIODO informed ZTM of the irregularities discovered in the course of the inspection and demanded that they be rectified. At present, the Inspector General is performing inspections in other cities in order to verify the scope of data processing carried out by other public transport companies that opted for ticketing systems similar to the one used by ZTM.

The ZTM audit case described above was the trigger for a larger audit conducted by the Inspector General at other public transport companies.

Social networks. In the first and second quarter of the year, the Inspector General conducted a series of checks on social networking sites. In the course of the inspections, it was established that, as a rule, the data controller is the website provider. The most commonly identified irregularity during the inspections of such entities was inadequate protection of the data collected on users' profiles. The process of logging in and editing the profiles was often weakly safeguarded (passwords too short and transmission of unsecured data). Organisational faults were made up of shortcomings in fulfilling the obligation to inform, lack of clear information on the possibility of reporting abuse, and imprecise regulations. As a result of the actions undertaken by the Inspector General, in cooperation with the administrator of "Nasza Klasa" (Our Classmate), a separate tab was created on the portal's website to show information on data protection issues and privacy threats, and introduced the functionality to enable users to set their data security level.

In 2009, the Inspector General conducted an inspection of the entities that are entitled to direct access to the National Information System so as to make an entry in the SIS and to access SIS data. The courts were the main subject of the inspection. The audits found many irregularities, such as lack of proper documentation (e.g. lack of a security policy) and that unauthorised individuals without the proper training have access to personal data. After the inspection and irregularities were found, the Inspector General asked the Minister of Justice to address the matter and correct the irregularities, particularly those related to the implementation of access to the Schengen Information System.

The Inspector General is continuing educational initiatives aimed at raising awareness among citizens about their right to data protection and privacy. Another educational project is a pilot programme aimed at

middle schools, "Your data - your business. Effective protection of personal data. An educational initiative aimed at students and teachers." The purpose of an educational initiative aimed at teachers and middle school students is to increase their knowledge of data protection and everyone's right to privacy protection. The program involves cooperation on the basis of a partnership between the self-government training centres for teachers and the General Inspector for Personal Data Protection. The pilot consists of two stages. In phase I, it was founded to train teachers, while phase II is the inclusion of the data protection matters into the teaching programs. The schools involved in the program will be provided with the outlines and student and teacher materials prepared by the Inspector General; an evaluation report will also be carried out on activities undertaken and the project of the nationwide educational program.

On 27 January 2009, as part of the 3rd Data Protection Day, the Inspector General signed an agreement with the Polish Bank Association entitled "Best practices for personal data processing in banks – from the perspective of practitioners" for the benefit of raising standards in personal data protection and in relation to the right to privacy in the banking activity. This agreement is intended to help create the code of best practices in data protection for the whole banking sector.

The Inspector General for Personal Data Protection in cooperation with the Episcopate of Poland developed the "Guidelines on Personal Data Protection in the Activity of the Catholic Church in Poland".

The Guidelines clarify the principles of proper safeguarding of personal data and are intended to help protect personal data in the activities undertaken by the Church, although the supervisory powers of the Inspector General are very limited as far as the operation of the Church is concerned.

Portugal

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

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

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

Directive 2006/24/EC (Data Retention Directive) was transposed into national law by Law 32/2009, entering into force in August 2009.

B. Major case law

The Central Administrative Court decided in favour of the DPA in a case in which the DPA did not authorise the Porto Municipality to carry out alcohol tests performed by non-health professionals on all their employees, and the results of which were delivered straight to the employee's manager.

The Court, in line with the DPA's arguments, considered that there was no reason to subject all employees to alcohol tests, except in some specific professional activities where the life of the employee or third parties might be at stake; any tests should be performed by health professionals (doctors or nurses) within the Service of Health and Safety at Work; the results of the tests cannot be communicated to the staff hierarchy but only state "able or not able to work".

In another judicial decision, resulting from an appeal against a DPA decision, the Administrative Court also ruled in favour of the DPA in maintaining the prohibition on setting up video surveillance cameras inside the editorial office of a TV station, where the journalists are working.

C. Major specific issues

General activity

The Portuguese DPA maintained its high level of activity during 2009. The number of data processing notifications was over ten thousand. Proceedings resulting from complaints, and investigations instigated at our own initiative came to more than seven hundred, and have resulted in the application of 260 sanctions for a total of 540,000 euros.

171 onsite inspections were also carried out, including an audit on the Voters Enrolment Database. As a result of these inspections, relevant recommendations were made and the implementation of these recommendations was monitored. The audit report was presented to the President of the Republic, Parliament and the Government.

The DPA initiated the implementation of the online notification procedure for specific data processing and continued the dematerialisation process of all documents, as well as the reform of the internal information system, leading to a quicker decision-making process in the short term.

Guidance to data controllers

In 2009, the Portuguese DPA issued guidelines to data controllers on some specific types of data processing with the following purposes: pharmacy surveillance, integrity lines (whistle blowing), credit transaction and recording of voice calls (call centres).

These deliberations provide guidance to data controllers on how to comply better with data protection rules, as well as to alert data subjects on their rights and on the conditions established for data processing.

With regard to whistleblowing, the DPA only allows a confidential system so as to prevent slander and discrimination; for limited purposes (prevention and repression of irregularities within accounting, internal accounting controls, auditing, fight against corruption and financial crime), and does not allow the reporting of any breaches of corporate governance; for specific categories of data subjects: reports should primarily be made against individuals who have responsibility

for decision-making in the above-mentioned areas. According to the DPA's understanding, these lines should be regarded as complementary optional mechanisms, subsidiary to the existing legal methods for reporting irregularities, with the employees clearly informed in advance of all relevant information concerning the data processing.

Opinions on draft laws

The DPA was asked, in 2009, to provide 86 Opinions on draft legal provisions containing data protection matters, either at national and international level.

At EU level, the most relevant one concerned the transposition of the Council Framework Decision 2006/960/JHA, the revision of the Regulation 1049/2001, the Council Framework Decision 2005/222/JHA, the amendments of Eurodac and Dublin II Regulations and the Draft Council Decision on the Customs Information System.

At national level, the DPA provided opinions on several bilateral agreements between Portugal and other States regarding exchange of information for tax and law enforcement purposes.

During 2009, the DPA also issued opinions on draft laws on the legal judicial regime in the context of health and safety in the workplace, on the right to information and informed consent in the health sector; on vehicle records, on electoral enrolment, and on the criminal investigation information system.

According to national legislation, the DPA must also provide opinions on the implementation of video surveillance systems operated by law enforcement authorities on public roads. In 2009, the DPA issued three negative opinions on the installation of such systems, considering that the legal requirements concerning proportionality were not met. In one case, the DPA provided a general positive opinion, but with limitations on the operation of the system during the night-time period. The DPA opinions are binding where they are not favourable. The terms of the authorisation are then set by the Ministry of Home Affairs.

DADUS Project

Developed by the DPA, this Project is aimed at children and young people from 10-15 years old and is applied in schools by including data protection and privacy matters in the curricula as part of the learning process.

In 2009, more than 2,000 teachers registered on the DADUS Project and the Project website and blog received over 200,000 hits.

The Project promoted three competitions on the theme of privacy: rap lyrics, a poster and a video. Participation was very high and the Project handed over the prizes at the schools.

The DPA has also signed an agreement with the Superior School of Cinema for the production of audiovisual materials by its students to be used within the DADUS Project to improve the multimedia component, which we consider to be one of the best ways of communicating with the youngest.

Romania

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

As in previous years, in 2009, the supervisory authority adopted decisions aimed at creating a standardised practice in accordance with EU regulations:

- in order to simplify the authorisation procedure and avoid excessive formalities, a Decision was issued establishing the model authorisation for the transfer of personal data to other countries.
- In order to ensure effective protection of the rights of data subjects, especially in the case of certain data processing operations that entail special risks for the individuals' rights and liberties due to the nature of the processed data, the purpose of the processing, the special character of the categories of data subjects or of the mechanisms used to process data, a Decision was issued establishing the personal data processing operations likely to present special risks for individuals' rights and liberties.

The supervisory authority was consulted as part of the process of drafting legislative acts on the processing of personal data, by a number of public authorities and institutions, namely the Ministry of Administration and Interior, the Ministry of Communications and Information Technology, and the General Secretariat of the Government.

In 2009, numerous data controllers and Individuals requested advice on the processing of personal data, thus demonstrating both an interest in ensuring the protection of personal data, and awareness of the impact that the processing of personal data has on one's private life. The most relevant of these points of view related to establishing the capacity of data controller and data processor, the disclosure of personal data and the processing of personal data within credit bureau-type filing systems.

B. Major case law

The courts' practice in litigation relating to the protection of personal data has maintained its standardised character. We would like to present below some of the relevant situations in which the sanctions imposed by the supervisory authority have been challenged before the law courts:

1. An investigation was carried out by the supervisory authority at a private company that processed personal data by providing street view services without prior notification, even though the processing had started in 2008. During that investigation, it was also noticed that no information was provided to data subjects with regard to the collection and later online publication of panoramic images containing natural persons, and that the data controller had not taken the necessary measures to ensure that the personal data in all images posted on the web site had been blurred.

   For these reasons, a fine was imposed. Unsatisfied with the findings in the record of the investigation, the data controller issued a complaint against it.

   The law court determined that the data controller had processed personal data without providing proper information to the data subjects with regard to the collection and uploading of the panoramic images containing personal data (individuals' faces, registration number plates of the vehicles passing by at the time the image was taken, as well as building numbers or names). According to the principle stating that the data must be adequate, relevant and non-excessive in relation to the purpose of the processing, these images should have been technically processed in such a way that they would not allow the identification of the persons in the frame at the time the panoramic images had been made.

   The law court, therefore, upheld the fine imposed by the supervisory authority on the data controller.

2. The supervisory authority noticed that a health care institution had not issued notification of the processing of personal data and had disclosed some

of the patients' data to other health care institutions without the consent of the patients and without any prior information being given.

As a result of these contraventions, the supervisory authority imposed fines.

The data controller contested the record of the investigation.

The court determined that the complaining patient had not provided his consent for the personal identification number of his son to be disclosed, this personal information had been disclosed afterwards to all medical offices within that county, and the data controller had not informed the data subject accordingly or issued notification of the processing of personal data.

The court maintained the sanction imposed by the supervisory authority in an irrevocable decision.

3. Following the investigation carried out by the supervisory authority on a public authority, it was noticed that the legal obligations on applying security measures and confidentiality of the processing of personal data had not been observed.

The public institution under investigation had posted on its website two regulatory acts approved by local authorities, which contained, among other things, tables with first names, surnames, personal identification numbers and data on the state of health (disabilities) of beneficiaries of certain facilities provided by law.

The disclosure of special personal data (articles 7 and 8 of Law no. 677/2001), even accidentally or by technical error, constitutes an infringement of the provisions of article 20 of Law no. 677/2001 by failing to ensure the adequate technical and organisational measures in order to protect personal data, as well as those of Order no. 52/2002 on approving the minimum security measures of processing personal data.

The law court upheld the sanction imposed by the supervisory authority.

C. Major specific issues

Romania's evaluation mission on personal data protection in view of its adhesion to the Convention Implementing the Schengen Agreement

Between 29 April and 1 May 2009, an evaluation mission in the field of personal data protection was carried out in Bucharest and was an extremely important event as part of the procedure of Romania's adhesion to the Schengen area.

The report of the evaluating experts contains favourable remarks with regard to the capacity of the supervisory authority to act independently, the high level of implementation of legislation on personal data protection and the effective cooperation of our office with other involved authorities. We would like to mention that the information campaign carried out in Romania by the supervisory authority, in collaboration with the General Inspectorate of Romanian Police and on a territorial level with the "Constantin Brâncuşi" Law School in Tg. Jiu and county police inspectorates, has been particularly appreciated.

The supervisory authority's president and staff attending the debates were congratulated on the professionalism and high standard shown in their activities, and for the organisation of the Schengen evaluation mission.

The Central and Eastern European Data Protection Authorities Conference

The supervisory authority hosted the Central and Eastern European Data Protection Authorities Conference, which is the annual meeting of data protection authorities in this area, constituting an excellent opportunity for debate and analysis of specific issues encountered within the activities of authorities with competences in the field of the protection of private life.

Representatives of data protection authorities from Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Poland, Slovakia, Slovenia as well as those of our supervisory authority as organisers attended this 11th meeting. General issues on the developments in the field of personal data protection registered in each country were debated, within the context of the relation between

the rights to private life, biometric data, the business environment, and new technologies.

The event, to which university professors and leaders of police units with experience in data protection were also invited to attend alongside data protection commissioners and experts from Central and Eastern Europe, constituted an excellent opportunity to identify and promote good practices in the field of personal data protection.

As regards the inspection activity, the budget restrictions imposed in 2009 caused the supervisory authority to change its strategy so that, apart from the investigations carried out with the competent authorities in view of Romania's adhesion to the Schengen area and the preliminary inspections carried out under the conditions of special law, solving complaints was considered a priority.

The complaints received by the supervisory authority related to receiving unsolicited commercial messages, reporting debtors' personal data to credit bureau type systems, and the illegal processing or disclosure of personal data.

In the cases found to have been grounded on the basis of the evidence received, infringement sanctions were imposed and it was decided, where applicable, to end the processing or delete the personal data processed without observing the data subjects' rights.

The complaints on unsolicited commercial communications referred to situations in which the data subjects received such communications via SMS messages and over the telephone without having expressed their explicit and unequivocal consent.

In addition to the general competency established under Law no. 677/2001, the supervisory authority exercises a number of powers set out under Law no. 506/2004 on the processing of personal data and the protection of private life within the electronic communications' sector.

The complaints sent to the supervisory authority on possible infringements of the right to private life through the processing of personal data within credit bureau-type filing systems generally related to the transmission of personal data without observing the individuals' rights and without their consent, or of the provisions of the Decision issued by the chair of the supervisory authority on the processing of personal data within credit bureau-type filing systems.

Slovakia

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

In 2009, the Office for Personal Data Protection of the Slovak Republic (hereafter referred as to "the Office") formulated new wording for some legal provisions of the Data Protection Act currently in force. The prepared draft law will amend the Data Protection Act taking into consideration recommendations resulting from the structured dialogue with European Commission representatives, incentives from the application of the Data Protection Act in practice, as well as the latest developments following the adoption of the Framework Decision on personal data protection processed in the framework of the police and judicial cooperation in criminal matters. The draft amendment will be submitted to the Slovak government in October 2010.

B. Major case law

In 2009, the Office was involved in several lawsuits. In two cases, the Office was subject to a judicial review of its decision to issue an order for a remedy imposed on an information system controller – and a credit provider processor. An order for a remedy was imposed on the controller in order to stop the unlawful disclosure of the payment demand disclosed in an open delivery letter. By these proceedings, the controller made data available revealing economic identity without legal grounds. The controller filed an action with the court in relation to this matter and, as of 2009, the ruling has not yet been finalized. In a related case, the court is involved in handling a petition of the processor of a former controller who claims that the respective Office's decision – an order to undertake an action for remedy which in this case means to proceed in accordance with the scope and condition of the personal data processing set up by the controller in a written contract – was not lawful. Again, this case has not yet been resolved by the final court judgment.

In the third case, the Office was subject to a judicial review of its decision to impose a fine on a controller. In particular, this controller did not adopt appropriate security measures. In the first instance, the county court was addressed, which decided that imposing a sanction was in line with the Data Protection Act. The controller referred the case to a higher instance by appealing to the Supreme Court. The case is still pending the decision of the Supreme Court.

C. Major specific issues

Inspection Activity and Issue of Notifications

Supervision of personal data protection in numbers

In 2009, data subjects and other natural persons who claimed a breach of the protection of their personal data filed 108 notifications with the Office. A further 36 notifications were filed by other subjects who alleged a suspected violation of the Data Protection Act. The Chief Inspector of the Office ordered 128 proceedings against the controllers of filing systems to be conducted ex-officio. In 2009, the Department of Inspection initiated 272 proceedings. Another 39 notifications were pending from 2008. Overall, in 2009, the Department of Inspection dealt with 311 notifications.

In this regard, the Department of Inspection, in coordination with the sub-department of investigation of complaints conducted 107 inspections and issued 72 'requests for explanations' to the controllers and processors of filing systems. Altogether 161 'orders' were issued for correcting the deficiencies determined by the inspection, which is a 120% increase compared to 2008. The right to file an objection against the issued order had been exercised by only four controllers, which amounts to just 2.5 % of the total number of controllers subject to the Office's orders.

In 2009, the Office imposed 19 fines for a total amount of 27,446.19 EUR. 12 fines were paid on time. In three cases, enforcement procedures are still underway. An intervention has been lodged by the controllers against the two Office's decisions in line with the Administrative Procedures. Two proceedings were initiated at the end of 2009 and in one of the two cases a reminder of the initiation of the administrative procedures was sent to the controller.

In 2009, 163 out of 272 new notifications were filed against private sector controllers and 55 against controllers from public administration, mainly against 'other public administration' bodies. In 31 cases, the

Office investigated notifications against autonomous authorities. 18 cases related to civil society organisations, foundations, political parties or movements and registered churches or religious groups. Public administration institutions were investigated in 5 cases.

Out of the 108 notifications filed by data subjects in 2009, the Office completed 85 cases, 66 of which were accomplished within the basic statutory period of 60 days, which is almost 78% of the total. The investigation of other notifications took longer for the following reasons: the need to consult other institutions, the need to inspect filing systems on a controller's premises, fact-finding that turned out to be more difficult, or the respective petitioners filed a request for cooperation. A total of 47 of all handled notifications were evaluated as being without grounds.

If a complainant is not satisfied with how his or her notification has been dealt with by the Office, he or she can re-submit notifications to the Office within the statutory period of 30 days. Out of 101 completed cases in 2009 (85 initiated and completed within 2009 and 16 initiated in 2008 and completed in 2009) only 7 repeat notifications were submitted to the Office. Six of them were dismissed in accordance with the Data Protection Act because they did not contain new facts. One repeat notification was examined by the Chief Inspector. This case was resolved by issuing a clarifying opinion. One repeat notification was filed after the mandatory period had elapsed. During 2009, the Department of Inspection filed one notification with law enforcement agencies.

Nationwide inspection activities of the Office

Inspections of the personal data processing performed by workforce agencies (head-hunters)

During 2009, the Office carried out several nationwide inspection operations. One of them was an operation targeting personal data processing by head-hunting (workforce) agencies.

Head-hunting agencies process not only data subjects' identification data, but also data revealing their professional skills and characteristics and details of their personality. This data is acquired mainly through a web interface or by regular post. During the inspections, the following main facts were examined:

- Legal basis for obtaining personal data,
- Compliance with the defined scope and purpose of the data processing,
- Information notice about the details of the data processing,
- Accuracy, integrity and updating of processed personal data,
- Duty to destroy personal data as soon as the original purpose of their processing has been fulfilled,
- Adoption of technical, organisational and personal measures to ensure protection of the personal data, including measures preventing risks of human failures by rendering advice to the 'entitled persons' authorised to access and process personal data.

By means of the inspections, it was established that controllers did not properly inform data subjects of their rights guaranteed by the Data Protection Act. The office issued an order setting out an instruction to all inspected controllers to rectify the shortcomings within a determined time period. In two cases, the Office lodged a proposal for imposing financial sanctions in administrative proceedings.

Inspections aimed at the processing of personal data by travel agencies

According to the 2009 Inspection Plan, travel agencies were also inspected. With the travel agencies, the Department of Inspection examined a similar set of questions as with the head-hunting agencies and also checked whether the content of the contracts with processors was compliant with the Data Protection Act.

Inspections proved that the reviewed travel agencies processed adequate personal data for the given purpose, destroyed them in the prescribed manner and, for the protection of personal data, they have taken appropriate technical, organisational and personal measures, except in one case. In this said case, it was proven that controllers obtaining personal data did not sufficiently inform data subjects about their rights guaranteed by the Data Protection Act.

All controllers gathered personal data of the data subjects through processors. In two cases it was found that contracts were not consistent with the provisions of the Data Protection Act because, for processors, they did

not define a list/scope of processed personal data and the conditions for their processing. Instructions were issued by the Office in order to eliminate the identified shortcomings. These instructions were all implemented.

Special inspection activities
In relation to the accession of the Slovak Republic to the Schengen area, in 2009, the Department of Inspection carried out further inspections in the selected embassies of the Slovak Republic abroad and in the relevant offices in the Slovak Republic. The aim of the inspections was to examine compliance of the controllers of filing systems with the Data Protection Act, procedures applied while issuing Schengen visas and meeting of requirements stated in the Schengen Catalogue (recommendations and best practices) related to issuing visas.

Inspections at the consulate departments of the Slovak Republic embassies in London and Dublin were carried out in May 2009.

In the third quarter of 2009, inspections were carried out in the following departments of Border and Aliens Police Bureau (BAPB) of the Ministry of Interior of the Slovak Republic: Border Control Unit Bratislava Ružinov - Airport, Unit for Coordination of Information Systems Operation of BAPB, Border Control Unit Vyšné Nemecké, Border Control Unit Košice - Airport, and Border Control Unit Poprad - Airport and Border Police Directorate Sobrance. In November 2009, an inspection was carried out at the Migration Office of the Ministry of Interior of the Slovak Republic and at the Accommodation Centre Rohovce focusing on processing of the personal data of asylum applicants.

Cooperation of the Department of Inspection with the foreign DPAs
In spring and autumn of 2009, the Department of Inspection participated in international workshops for inspectors of the personal data protection authorities. At the XIX Workshop in Prague in March 2009, the Department of Inspection presented its contribution to the topic "Processing of personal data in the area of healthcare". At the autumn working meeting of inspectors in Limassol in October 2009, the Office presented its experience gained from inspections on the processing of personal data by employers, including copying and collecting of official documents.

In November 2009, the Office's employees participated in the Francophone Conference on Privacy and Personal data Protection in Madrid, which was organised by the Association of Francophone Data Protection Authorities. High on the conference agenda was the protection of personal data in the digitalised world and the protection of children's privacy. After the conference, the Office representatives took part in the General Assembly of the Association of Francophone Data Protection Authorities.

Cross-border Personal Data Flow
In 2009, the Office issued eight approvals of cross-border personal data flows to countries that do not provide an adequate level of data protection. In the case of one multinational company, approvals of personal data transfers were issued on fulfilment of the adhesion requirement of data importers to the Safe Harbour principles and, in the remaining cases, through application of the standard contractual clauses for processors in third countries in the respective contracts on personal data transfer. There have also been cases in which the controller – multinational company applied both the Safe Harbour scheme and the standard clauses designed for processors in third countries not ensuring an adequate level of data protection. The subject of cross-border data flows mainly related to personal data about employees and clients of international corporations.

During 2009, the Department of Foreign Relations issued 48 written opinions to questions submitted by the controllers of information filing systems, or by the law firms representing the controllers of information filing systems. Questions were mostly related to the transfer of personal employment data, human resources management, whistle-blowing and processing of the personal data of controllers' clients.

Questions were aimed at clarifying the cross-border personal data flow conditions between:
- Controllers and processors based in EU countries,
- Controllers and processors based in India and the Republic of Korea,

- Controllers and processors based in EU countries with the onward transfer to a third country that does not provide an adequate level of data protection,
- Cross-border data flow for the purpose of whistle-blowing.

International Cooperation

Tasks at the international level resulted mainly from the Slovak Republic's membership of the European Union and in working groups established under its auspice and from legal acts of the European Communities. Particular obligations arose from the membership of the Slovak Republic in Europol, Schengen Information System, Customs Information System, Working Group on Police and Judicial Cooperation, Coordination Working Group for Eurodac and Schengen Evaluation Working Group (SCHEVAL). In compliance with the working programme for 2009 prepared by the European Commission and the Standing Committee on the Evaluation of Schengen States, the Expert Group SCH-EVAL conducted:

- A review of the enforcement of underlying principles for the processing of personal data in SIS by 'old Schengen states' (Germany, France, Belgium, the Netherlands and Luxembourg),
- A review of preparedness to implement the Schengen *acquis* in the field of protection of personal data in the candidate countries - Bulgaria and Romania.

The findings and recommendations outlined in the evaluation reports revealed, on the one hand, limitations in the practical application of the SIS Convention and, on the other hand, a responsible approach of the evaluated candidate countries while attempting to meet the criteria required for entering the "Schengen area". Final evaluation reports were submitted to the Working Group for SIS / SIRENE and the Council for its approval.

Within the framework of bilateral and regional meetings held to address specific issues of cooperation and to exchange best practices, the most important are as follows:

- Participation at the 11th meeting of the supervisory authorities for data protection in Central and Eastern Europe (DPA of EEC countries) in May 2009,
- Meeting with EDPS, Mr Peter Hustinx, on the premises of the Office in September 2009. Mr Hustinx was thoroughly informed about the Office's activities and discussed challenges and new priorities with the employees of the Office on data protection in the European Union as well as the possibility of achieving the best possible synergies of efforts between the supervisory authorities for data protection. Mr Hustinx also visited the National Council of the Slovak Republic where he met members of the Parliamentary Committee on Human Rights, Minorities and the Status of Women. On this occasion, a special press conference was organised which was devoted to his visit to Slovakia,
- A thorough exchange of best practices on mass media policy, raising awareness and opportunities for cooperation with the Office of Personal Data Protection of the Czech Republic in Bratislava in October 2009.

Slovenia

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

In Slovenia, the modern legal and institutional framework for data protection (and access to public information) has been established and has been consistent with the *acquis communautaire* for years.

In accordance with the special provision of Article 48 of the Personal Data Protection Act[22] (PDPA), the Information Commissioner issued several preliminary opinions on preparatory legislation in relation to compliance with personal data protection. The Information Commissioner's main achievements include the amendments and supplements to the Electronic Communications Act[23] (ECA) passed at the end of 2009. The amendments include the provision on anonymisation of telephone numbers included in the itemised bills received by subscribers as provided by the e-Privacy Directive (2002/58/ES). The recommendations of WP29 (WP 113) regarding the provisions of the Data Retention Directive (2006/24/ES) were also taken into account. The data retention period is now shortened to 8 months and must not exceed 14 months. The amended ECA also limits the retention period for the supplied retained data and also brings the registration of supplied retained data down from an indefinite period to a limited period of 10 years. One of the most important changes to the ECA is the provision on supply of traffic and location data to the police in the event of life and limb protection and on the Information Commissioner's competence to oversee the provisions on lawful interception of communications.

The other major pieces of legislation considered by the Information Commissioner in 2009 included laws concerning general administrative procedure, criminal procedure, foreigners, passports, state border, banking, foreign affairs, health, police, Red Cross, family code, money laundering and terrorist financing prevention, and archives.

B. Major case law

Similar to previous years, in 2009, the Information Commissioner dealt with several cases widely publicised by the national media.

Political parties
The Information Commissioner initiated an inspection procedure against two political parties in Slovenia because of suspected illegal collection and retention of personal data for the purpose of electoral campaigning. The complaint came from a number of Slovenian citizens/registered voters living abroad, who received direct marketing material from the two political parties without having given their consent to the parties to use their contact data for marketing purposes. In the course of the inspection procedure the political parties could not prove a legal basis for the collection of the citizens' contact data. As a consequence of the established violation the Information Commissioner fined the two parties € 4,170 each. The liable persons in the parties were also fined € 830 each.

President of the District Court
The President of the District Court was found liable to pay a fine of € 1660 for two offences of unlawful processing of personal data. It was established in the offence proceedings that the liable person had been collecting and further processing data on calls made from work telephones (traffic data) of two employees. The purpose of processing this traffic data was not defined or lawful, and further processing was not consistent with the law. The Information Commissioner's decision is not yet final. Pursuant to the provisions of the Courts Act, the Higher Court also conducted an inspection of the work of the court management at the aforementioned District Court.

Since this case merely reflects widespread problems in the field of privacy in the workplace, the Information Commissioner once again expressed its view that this field requires an improved legal framework as practically one third of all cases in the Information Commissioner's competence touches upon workplace privacy.

[22] Official Gazette of the RS, No. 94/2007

[23] Official Gazette of the RS, No. 13/2007

Unlawful supply of personal data between two insurance companies

The Information Commissioner fined two insurance companies and the liable individuals for unlawful processing of personal data. In the proceedings, the Information Commissioner established that personal data of 2382 individuals had been supplied without legal basis provided by law or personal consent of the affected individuals.

The insurance company that supplied the personal data was fined for unlawful supply of personal data and for insufficient traceability of the supplied data. The Information Commissioner found conclusive evidence that data on 26 individuals had been processed unlawfully and, therefore, the company was fined € 112,590 and the liable person was fined € 20,000. The company filed a request for judicial review. The other insurance company was fined € 108,420 for unlawful acquisition of personal data, and the liable persons were fined € 20,000 each. This company took advantage of the option provided by law and paid half of the fines immediately.

These are the highest fines imposed by the Information Commissioner so far. The Information Commissioner emphasised that in the future such unlawful supply of personal data among the controllers that are in possession of sensitive personal data or of large databases will be strictly sanctioned.

Data protection in banks

The Commissioner conducted a systematic inspection of personal data security in the banking sector (6 of the biggest banks), namely the lawfulness of processing personal data in the inter-bank transfers of client credit rating data included in the new SISBON system, and the lawfulness of access to clients' bank account data. The Information Commissioner established that in the context of inter-bank data transfers, no data had been accessed unlawfully. However, unauthorised access to the data of some well known clients' (politicians') bank accounts had occurred in two of the banks included in the inspection. The unauthorised employees who accessed the data of clients' bank accounts were sanctioned pursuant to the General Offences Act.

Journalist's e-mail and questions published on the Information Commissioner's website

On its website, the Information Commissioner published an e-mail received from a journalist containing journalistic questions and the journalist's work e-mail address. The journalist's e-mail was also sent to a number of subscribers on the Information Commissioner's mailing list. The journalist filed a complaint; however, the Information Commissioner found no breach of the Data Protection Act and did not initiate an inspection procedure. The reasoning of the Information Commissioner was that the e-mail was sent to the Information Commissioner's official work e-mail address, established to receive e-mails from natural and legal persons concerning the work area of the Information Commissioner. The first name, surname and work e-mail address of the journalist in this case did not represent protected personal data, as the journalist was acting in his public journalistic role, with his name published on the official website of the media. His privacy and dignity were, therefore, not prejudiced by the publication of his e-mail. The questions contained in the e-mail concerned the public nature of the Information Commissioner's work and, in addition, the contents of the communications were intended for publication. This is why the journalist's questions could not be regarded as a protected personal communication but rather as public information.

A judicial decision published in the newspaper

A part of a judicial decision containing the plaintiff's personal data was published in one of the Slovenian dailies. The Information Commissioner found a breach of the Personal Data Protection Act and fined the newspaper company and the liable person. The case is important because the Information Commissioner took the position that personal data contained in a judicial decision pertaining to a non-public figure represents protected personal data. The judicial decision may, therefore, only be published in anonymised form. The Information Commissioner also took the position that in the event of a conflict between the right to freedom of expression and the related constitutional principle of publicity of trial and the right to data protection, in this case the right to data protection of the non-public figure prevails. The public interest is not the same as what

the public is interested in and the sole curiosity of the public must not justify intrusions of the constitutional right to information privacy.

C. Major specific issues

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

Since **biometric measures** can only be performed following approval of the Information Commissioner, a total of only 10 applications were received in 2009 (compared with 16 in 2008 and even 40 applications in 2007). Proportionally, a decrease was noted in the number of decisions issued – 6 decisions (4 granted, 2 refused) compared with 17 decisions in 2008 and 35 decisions in 2007.

The situation relating to the grant of permits to inter**connect filing systems** was unchanged in 2009: a total of 8 decisions were issued both in 2009 and 2008 (7 in 2007) regarding the connection of filing systems.

In 2009, 71 complaints were lodged with the Information Commissioner as a competent body for deciding on the appeal of a data subject concerning the **right to information**.

By the end of 2009, the personal data filing systems of more than 11,000 controllers were registered in the **Public Register** managed by the Information Commissioner and published on its website. The figures show an increase of about 1,000 new entries per year.

In the framework of its **inspection activities** (as of December 2009, there are nine state supervisors for data protection - inspectors employed with the Commissioner), in 2009, the Information Commissioner received 624 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act, including 219 (256 in 2008) in the private sector and 405 (379 in 2008) in the public sector. Compared with previous years (635 cases in 2008, 406 cases in 2007 and 231 in 2006), the sharp rise in caseload to the extent of 76% in 2007 and 56% in 2008 has now declined. Similarly to previous years, most complaints pertained to unlawful or excessive collection of personal data (PD), disclosure of PD to unauthorised users, illegal video surveillance, insufficient PD protection, unlawful publication of PD, and so on. Administrative offence proceedings were initiated in 163 cases (279 cases in 2008 and 133 cases in 2007).

In 2009, the number of requests for **written opinions** and clarifications amounted to 596 written answers and 1471 short answers from the Information Commissioner (as well as several hundred verbal answers by phone). In light of the figure of 853 cases in 2008 and 1144 cases in 2007, these figures clearly reflect the sustained high level of public awareness of the right to privacy brought into effect by a modern Personal Data Protection Act and also by the transparent work and intensive public campaigning of the Information Commissioner.

In addition to publishing non-binding opinions in the form of written explanations on its website and publishing a number of brochures on matters of data protection, in 2009, the Commissioner continued to publish **guidelines** on specific matters of data protection. The purpose of the Information Commissioner's guidelines is to provide common practical instructions and information to the public, data subjects and controllers in a form of typical frequently asked questions and answers to comply with the statutory provisions of the Personal Data Protection Act and/or other legislation. Last year, the Commissioner prepared and published guidelines on its website regarding the code of conduct in handling personal data collection, protection of personal data in relation to the media, informing and raising awareness of the consumers, identity theft, data protection of children in school, prevention and protection from cyber bullying, and social engineering.

In the context of the Third European **Data Protection Day,** which celebrated its 3rd anniversary in 2009, the Commissioner organised a roundtable debate on the topic of "Privacy in the workplace". For the third time, the Commissioner awarded subjects from the public and private sectors for good practices in personal data protection. The awards for excellence in data protection were presented to the company Cetis d. d. and to the Ministry of Defence of the Republic of Slovenia. In

addition, for the first time, awards were presented to companies that proved a high level of personal data security with an ISO/IEC27001 certificate for information security.

International cooperation

Permanent cooperation in the bodies of the European Union and the Council of Europe

The Information Commissioner, as the national regulatory body in the field of data protection, permanently cooperates with the competent bodies of the European Union and the Council of Europe in the field of data protection. The Information Commissioner is bound to international cooperation by the provisions of the Directive 95/46/EC.

In 2009, the Information Commissioner actively participated in five working groups at EU level, concerning supervision of data protection in the EU in different areas. These encompass the working group for the protection of personal data under Article 29 of the European Data Protection Directive, the joint supervisory bodies for Europol, the Schengen area and the customs information system, as well as the coordination meetings of the European Data Protection Supervisor together with national bodies for the protection of personal data and supervision of EURODAC.

In 2009, the Information Commissioner was elected deputy chairman of the joint supervisory body for Europol, and within the scope of police and judicial cooperation the Commissioner regularly attended meetings of the Working Party for Police and Justice.

With the entrance of Slovenia into the Schengen area, the Information Commissioner became the independent body overseeing the transfer of data for the purpose of the convention and its competencies were extended to include oversight of Article 128 of the Schengen Convention. In 2009, 55 requests for access to personal data were received and none of the requests were denied. The Information Commissioner has not received any complaints regarding the execution of the right of individuals to access their data contained in SIS at the first level.

In 2009, the Information Commissioner participated in the inspection supervision group for the Schengen evaluation of Bulgaria and Romania to enter the Schengen area in the framework of SCHEVAL.

In the context of the Council of Europe, a representative of the Information Commissioner participated in the Council of Europe's Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). This year the Council mostly worked on the Draft recommendation on the protection of individuals with regard to automatic processing of personal data in the framework of profiling.

The Information Commissioner also actively participated in the Internet and Information Technology Sub-Group under the auspices of the European Data Directive Working Group. The working group adopted two important documents in 2009, namely the Recommendation on Data Protection and E-Waste and Report and Guidance on Road Pricing – "Sofia Memorandum". The Sofia memorandum was initiated at the recommendation of the Slovenian Information Commissioner. The international working group IWGDPT continues the work in fields such as Deep Packet Inspection, geolocation data, social networking sites and others.

Other international cooperation

The Information Commissioner's representatives have also participated in the following important **international events**:

Barcelona conference "High level meeting for joint proposal to draw up international standards on privacy and data protection"
Spring Conference on personal data protection, Edinburgh
2nd European Privacy Open Space and "re:publica", Berlin
Data Protection Conference 2009, Brussels
11th Meeting of the Central and Eastern European Data Protection Commissioners, Romania
Open Society Institute Meeting on Freedom of Information, Budapest
Strengthening Data Protection in Israel, Tel Aviv (twinning project)

International Conference of Information Commissioners, Oslo
10th Case Handling Workshop, Limassol
Third Privacy Open Space Conference, Vienna
31st International Conference of Data Protection and Privacy, Madrid.

The Commissioner built on **bilateral cooperation** mainly with Hungary, Serbia and Montenegro.

All these efforts and achievements have also resulted in the high rating the Commissioner permanently enjoys in terms of reputation, public trust and public awareness of its activities, which is also reflected in the findings of public opinion polls. According to the latest results (January 2010) of the survey on public trust carried out by the Slovenian Public Opinion Research Centre, trust in the Information Commissioner is evidently growing. Among other measured institutions, the only institution that is more trustworthy than the Information Commissioner is the official currency, the Euro. With a high degree of public trust (53.1 %), the Commissioner came head and shoulders above all other institutions, such as the Military, the President of the Republic, the Ombudsman, Schools, and Police. It is also worth mentioning that the Information Commissioner enjoys the lowest rate of public distrust among all the institutions included in the survey.

In May 2009, at the proposal of the President of the Republic, the National Assembly of the Republic of Slovenia elected Mrs Nataša Pirc Musar for another 5 year term as the Information Commissioner with the vast majority of votes.

Spain

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

During 2009, the following regulations relating to data protection matters were adopted:

1. Act 25/2009, dated 22 December, which amends several acts in order to adapt them to Act 17/2009, on free access to service activities and their exercise.

   This act amends the Private Security Act, among others, and liberalises the selling, delivery, implementation and maintenance of many security services, including video surveillance systems. Before the enactment of this act, the installation of such devices was only lawful, pursuant to the Data Protection Act, when performed by companies accredited by the Ministry of the Interior. Moreover, the installation contract had to be notified to the Police. These formal requirements are no longer in force.

2. Act 29/2009, dated 30 December, which amends unlawful competition and advertising regulations in order to improve the rights of consumers and users.

   Without prejudice to the provisions of data protection rules and information society services and telecommunications rules, this Act states that repeated unsolicited communications for direct marketing purposes, by means of electronic mail or equivalent means, will be deemed as unfair conduct, except in circumstances legally justified to enforce a contractual obligation.

Furthermore, the Spanish Data Protection Agency (AEPD) has continued to work towards greater legal certainty and a national legal system consistent with data protection law. More than 100 reports were issued by the legal department, as required by the Data Protection Act, concerning the adoption of general provisions such as:

- Draft for the Bill on the prevention of money laundering and terrorist financing, which has been postponed twice.
- Draft for the Bill on sexual and reproductive health and abortion.
- Draft for the Royal Decree adopting the minimum set of data to be included in clinical reports in the National Health System.

Draft provisions implementing Act 11/2007, dated 22 June, on electronic access by citizens to public services, which transposed Directive 2006/123/EC into Spanish law.

B. Major case law

Before analysing the specific judgments by Spanish courts, it is important to mention that a significant number of rulings concerning the issue of the right to erasure from the baptism books of the Catholic Church have been made, all of them consistent with ruling 4646/2008 of the Supreme Court, dated 19 September, explained in greater detail in the Twelfth Annual Report of the Article 29 Working Party. For that reason, the following analyses were carried out without taking these rulings into account.

National Court

In 2009, the National Court of Spain ruled on 240 appeals to overturn decisions adopted by the Spanish Data Protection Agency, 162 of which were fully rejected (68%). Regarding upheld claims (17 partially and 61 wholly), it should be noted that many of them were based on different interpretations of evidence, and not on application of law. The following rulings should be highlighted:

- Ruling of 17 March, the first to ever deal with an appeal against a decision that did not authorise a transfer of personal data to a third country.
- Ruling of 22 April, which found that recording a person without his consent on a video file stored on a CD, to be used in a trial as evidence, is outside the scope of the Data Protection Act, because such data does not form part of a filing system and is not intended to form part of a filing system.
- Ruling of 9 July, which found that the publication by a newspaper of images of a terrorist attack victim with irreversible brain damage was disproportionate, and gives priority to the right to data protection with respect to the right to freedom of information.
- Ruling of 9 October, which clarified that filing systems owned by prosecutors are subject to the Data

Protection Act, and, therefore, to the supervisory powers of the Spanish Data Protection Agency.
- Ruling of 26 November, which confirmed the penalties imposed by the Spanish Data Protection Agency on a company that processed the personal data of a minor, without his parents' consent, to offer him a credit card as part of a direct marketing campaign.

Supreme Court

For its part, the Supreme Court confirmed the criteria of the Spanish Data Protection Agency in 16 of its 19 judgements dealing with the decisions of said Agency, including:
- Ruling of 28 April, which stated that Spanish law applies to a filing system stored in a server located in the United States, whose data is processed to carry out an advertising campaign managed by a Spanish company and targeting Spanish citizens.
- Ruling of 17 November, which confirmed that the derogation allowing the disclosure of personal data to courts, only applies when such Courts directly ask for the data.

Decisions by the AEPD

The number of claims brought before the Agency in 2009 caused an increase of 75% in the actions brought, exceeding 4,100 (of which telecommunications, financial institutions and video-surveillance were the main sectors investigated). However, in decisions on sanction procedures against private organisations, telecommunications and financial institutions, despite occupying the first and third place based on the number of proceedings, saw a decrease of 10.34% and 21.26% respectively. On the other hand, private video surveillance for security reasons rose to second place, with 229.55% growth on the previous year. Furthermore, in an environment of economic crisis such as that which developed during 2009, there has been an exponential increase in actions derived from or related to claims for default. Decisions that declare a breach of the Data Protection Act by Public Administrations increased by around 12.5%.

The number of the sanctions imposed came to 24,872,979.72 euros. Although this figure represents an increase of 12.99% compared with the previous year, it is close to the volume of sanctions declared in 2006, with the relevant difference that the number of sanction procedures resolved in 2009 is higher than that of 2006 by 235%. It is precisely the considerable increase in sanction procedures and not the sum of the sanctions declared that explains the figure of the sanctions imposed. Minor sanctions are those that present the greatest increase (44.76%), whilst serious ones remain stable and very serious sanctions decrease by almost 6%. Regarding the total of the sanctioning decisions, a marked reduction of the liability of the offenders can be seen in 40.72% of the cases. Analysing the data presented, it is appropriate to conclude that the quantitative increase in the sanctions, a consequence of the previous increase in complaints, does not detract from an appreciation of the improved compliance with the Data Protection Act (with the growth in the number of breaches being for reasons of form), the reduction of very serious breaches and the reduction of liability when a breach is committed.

In any case, it is worth highlighting the following resolutions:
- Decision PS/00053/2009, dated 13 January. The Information Commissioner's Office (UK) reported to the AEPD that a Spanish company was making unsolicited commercial calls (cold calls) to British citizens. The company was not able to demonstrate the origin of their data, and it never had any contractual relationship with the data subjects and had not asked for their consent. The Agency, therefore, imposed a fine of 60,001 euros for a serious breach of the Data Protection Act.
- Decision PS/00593/2008, dated 20 April. A database with medical data from 140 workers had been found through a P2P file-sharing program. The controller, a company specialising in occupational risk prevention, tried to lay the blame at the door of a former employee. The Agency fined it 60,001 euros for not having implemented the appropriate security measures, which is a very serious breach of the Data Protection Act.
- Decision PS/00183/2009, dated 14 September. An online ticket store offered two concert tickets to the user who managed to forward a specific advertisement the most number of times. The Agency found that the store sent unsolicited commercial communications, and fined it 30,001 euros for a serious breach of the Information Society Services Act.

- Decision PS/00233/2009, dated 20 October. A telecommunications company sold clients' defaulted debts to third companies. Non-existent, uncertain or disputed debts were included in the database, and were even added to the credit histories of some data subjects. The Agency fined it 420,000 euros for a very serious breach of the Data Protection Act.
- The full text of the decisions adopted by the Spanish Data Protection Agency may be found at https://www.agpd.es/ (in Spanish).

C. Major specific issues

Facilitating compliance with the law: a guarantee for citizens. The Agency's awareness raising policy was strengthened in the conviction that facilitating compliance with the law results in an increase in the guarantees to citizens. Thus, in January 2009, the 2nd Annual Open Session was held, which was attended by around 700 participants, and the catalogue of practical guides was expanded, publishing new editions with recommendations to Internet users, video-surveillance and data protection in the workplace and, in English, guides on video-surveillance and the rights of boys and girls and the duties of fathers and mothers.

The Helpline continues to be a very useful channel in the informative policy of the Agency, as is shown year after year by the increase in consultations. The Legal Department, for its part, dealt with a total of 679 consultations, of which 359 (54%) were made by the Public Administrations and 313 (the remaining 46%) by the private sector.

These policies continue to give results. In 2009, almost 400,000 files were registered in the General Data Protection Register (RGPD), which implies an increase of over 50% compared to 2008, reaching a total figure of 1,647,756. One contribution to this increase has been the simplified notification system NOTA, which facilitates notification via the Internet, something which is used in almost 90% of manual notifications. Furthermore, the use of digital certificates is gaining ground, to the point that this format is used in one in five notifications.

The increase in registrations is strongest in the private sphere, which has grown by 63%, whilst in the public sector an increase of almost 50% can be highlighted in Local Administration files, owing to which the files of municipalities in the RGPD represent almost 96% of the Spanish population.

The offer of new channels to facilitate compliance with the law has led to a qualitative leap in the EVALÚA programme, an online self-test for self-assessment of compliance with the LOPD for companies and local authorities, which offers answers free of charge to the queries commonly experienced by those who process personal data.

Internet. New services, new challenges. The consideration for the free use that users make of Internet services is the unilateral establishment of terms and conditions by the service provider. Therefore, priority should be given to those active policies aimed at establishing relations with the providers of these services. In this respect, the AEPD has communicated the recommendations of the study prepared with INTECO to Facebook and Tuenti, insisting on the improvement of privacy policies so that they offer clear and understandable information, and on the need to set up default privacy policies and erase all the contents of the profile as soon as deregistration is requested.

In 2009, 156 proceedings were brought regarding preliminary proceedings specifically related to services provided via the Internet. A new aspect relates to the fact that 18 of these proceedings were instituted as a consequence of 31 complaints related to users of the social networks Facebook and Tuenti, the majority referring to the dissemination of photographs of third parties without their consent.

The majority of the remaining actions also related to the unauthorised dissemination of personal data via the Internet: 37 of them refer to forums or blogs, 13 to video hosting services, basically Youtube, and 38 to other types of website such as corporate sites, collections of law reports, and personal sites. Another 28 claims related to advertisement websites, online dating services or e-mail services. Most cases are related to the unauthorised dissemination of data.

Likewise, 10 of the actions dealt with incidents of various types related to online shopping or electronic commerce operations. Finally, it is worth mentioning five preliminary

proceedings brought in relation to web search engine services and the location of personal information in directories or people search engines.

Minors. Necessary protection in light of their growing presence in the Web: The use of social networks has become a habitual activity for the social development of minors, who are provided with a new means of contacting each other. The risk for them is that, to a great extent, they start out with a basic educational deficit regarding how to exercise real control over their information.

Data protection regulations do not allow minors under the age of fourteen to register as users of a social network without the consent of their parents. The Agency assumes compliance with this obligation as a priority. In fact, in the meetings held with those responsible for Tuenti and Facebook, access control for minors was an ongoing demand.

In response to the demands of the AEPD, Tuenti presented an age verification system that analyses the profiles of suspect users, erasing those who do not prove that they are 14 years old. Likewise, it has undertaken to strengthen the purging processes of existing profiles and to develop systems for the verification of new suspect profiles. Furthermore, it has issued information regarding the modification of the privacy policy, setting the maximum privacy level as the default for users under the age of 18. Likewise, the Agency requested those responsible for Facebook to increase the age limit to 14 years for users in Spain.

However, it is necessary to incorporate adequate training on data protection and privacy into school books, and for Public Administrations and schools to make technologies available to pupils that limit access to web services by children under the age of 14. In this context, the electronic Identity Document is proving to be one of the most efficient instruments for accrediting age on the Internet. This Agency considers it to be extremely important that the adequate initiatives be implemented in order for over-14s to have the digital means available to allow them to prove that they have the required age to give their consent to the processing of their data.

Video-surveillance: living with guarantees. Video surveillance for security reasons has become an omnipresent reality. Each year sees significant growth in video surveillance files, as in 2009, when such files registered in the General Data Protection Register increased by around 240% (an increase of more than 37,000 files) in the private sphere. In the public sphere, there was an increase of 60% (an increase of 578 files).

The 2009 survey of the CIS shows that 68.7% of citizens are in favour of video surveillance installation, whilst 10% are against it. However, an increasing number of people are lodging complaints regarding breaches of the LOPD in relation to video surveillance, where the resolved sanction proceedings have increased by 230%.

With regard to cameras that allow images to be transmitted via the Internet, the AEPD carried out a sectoral inspection, noting that the majority allow the persons filmed to be identified. The main deficiency detected is that the control mechanisms for access to the images are often disabled by the manufacturer or enabled with a default username and password. The lack of diligence in access control causes a vulnerability that allows third-party access by leaving the camera in an "open door" situation. A catalogue of recommendations is offered, including the need to enable image access control by means of usernames and passwords. As a result of the inspection, seven sanctions proceedings were opened and resolved.

Employment context: the balance between rights and obligations. The range of personal data processing carried out in the employment sphere has led the AEPD to prepare a guide on data protection in companies, to provide answers to practical aspects that companies are commonly faced with, suggesting criteria to ensure compliance with personal data protection regulations. The guide includes specific recommendations on the processing of specially protected data, in particular, data relating to healthcare and trade union membership, as well as the guarantees that should be observed in occupational risk prevention.

Although not necessarily dealing with personal data, it also incorporates recommendations to ensure that the implementation of internal whistleblowing schemes

in the company is carried out while guaranteeing the protection of the employees. The chapter dedicated to employer inspections indicates the rules applicable to biometric controls, video surveillance in the workplace or the use of technological tools provided by the employer and also control of occupational absenteeism.

International data flows. Flexibility and globalisation. International data transfers from Spain have become globalised and now reach all corners of the world. The number of authorisations increased by 25%, the USA being the first destination country, despite the reduction in the number of transfers. There has been strong growth of 100% to Latin American countries (132 authorisations), whilst Asia maintains a constant volume of authorisations (115). On the African continent, international transfers focus on Morocco (19) and the Republic of South Africa (3), and Australia appears to be an emerging destination.

The search for more flexible procedures for the authorisation of international transfers saw progress in 2009. The AEPD authorised the first transfer based on binding corporate rules (BCR) and participated via a coordinated procedure in ten requests with this type of guarantee presented before other authorities in the European Union.

To conclude, it can be affirmed that we are witnessing a constant increase in international data flows with a focus on delocalisation of services and more flexible authorisation procedures. From this, we can deduce the urgent need to achieve binding standards to guarantee the protection of privacy in a globalised world.

2009: Madrid, World Privacy Capital. The Madrid Resolution: a meeting point for a global regulation. In 2009, the AEPD organised the 31st International Conference on Data Protection and Privacy Authorities – the largest forum dedicated to privacy at world level and a meeting point for data protection authorities and guarantors of privacy coming from all over the world, as well as representatives of public and private bodies and civil society – making Madrid the world privacy centre between 2 and 6 November. It was attended by more than 1,000 people from 83 countries.

This Conference, inaugurated by their Highnesses the Prince and Princess of Asturias, took place in the Congress Palace of Madrid, under the slogan "Privacy: today is tomorrow". There were nearly one hundred speakers, participating over twenty sessions, including Alfredo Pérez Rubalcaba, the Spanish Interior Minister, Janet Napolitano, the Secretary of Homeland Security of the United States, Martin Cooper (inventor of the mobile telephone), Vinton Cerf (co-inventor of the TCP/IP family of Internet protocols), and Ahmed Reda Chami. the Minister of Industry, Commerce and New Technologies of Morocco. However, the greatest achievement of this event was the progress made towards a universal and binding legal instrument on the subject of privacy, contributing to greater protection of individual rights and freedoms in a globalised world and benefiting from the widest institutional and social consensus.

On adopting this "Madrid Resolution", a large step was taken towards the "Joint proposal for a Draft of International Standards for the Protection of Privacy with regard to the Processing of Personal Data". This proposal aims, firstly, to promote the right to data protection and privacy internationally, offering a model of regulation that guarantees a high level of protection and which, at the same time, may be assumed in any country, and secondly to facilitate the flow of personal data at international level while helping to overcome the existing obstacles.

Despite not being an international agreement or a legally binding regulation, its value as a reference text is justified not only by the wide participation of the international data protection and privacy community in its preparation, but also because it includes elements that are present in all the valid data protection systems currently in force, and because it has been backed by all the Authorities that attended the International Conference. Therefore, the promotion and dissemination of this text among private bodies, experts and national and international public organisations will be one of the priorities of the AEPD during the year 2010.

Sweden

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

Directive 95/46/EC is transposed into Swedish law as the ***Personal Data Act*** – PDA – (1998:204) which came into effect on 24 October 1998. The PDA is supplemented by the ***Personal Data Ordinance*** which came into effect on the same day. The Act applies, as with the Directive, to automated processing as well as manual processing. Even though the Act, in principle, applies to processing of personal data in all sectors of society, there are specific Acts and Ordinances that apply to processing of personal data in certain activities, either instead of, or in addition to, the PDA. Also in drafting these specific Acts and Ordinances, the Directive has been taken into account.

Directive 2002/58/EC is transposed into Swedish law as the ***Electronic Communications Act*** – ECA – (2003:389) which came into effect on 25 July 2003. In chapter 6, the ECA provides rules on data protection in the electronic communications sector. Compliance with the data protection rules in the ECA is supervised by the Swedish Post and Telecom Agency (PTS). Article 13 of the EC Directive regarding unsolicited e-mail is transposed into Swedish law as amendments in the ***Marketing Practices Act*** (1995:450). The amendments came into effect in April 2004. The Marketing Practices Act falls under the supervision of the Swedish Consumer Agency (Konsumentverket).

Ipred *(Intellectual Property Rights Enforcement Directive)* has been transposed into Swedish law through different amendments to national laws which came into force on 1 April 2009. The amendments make it easier to investigate suspected cases of illegal file sharing. One specific feature of the legislation is that organisations protecting intellectual property – if they suspect that someone has engaged in illegal peer-to-peer file sharing – may turn to a court of law and require that Internet providers disclose information about the IP address owner. There have already been a few trials and one case is now pending in the Svea Court of Appeal.

As of 1 December 2009, the National Defence Radio Establishment (FRA) gradually started collecting intelligence via cable according to the ***Signals Intelligence Act*** which came into effect on the same day. This new Act entitles the FRA to collect intelligence both over the airways, i.e. targeted at radio signals, and via cable. Until the new Act entered into force intelligence via cable could not be collected. However, an increasing proportion of international traffic, where the interesting information is found, is now transmitted by cable, so it was necessary to introduce technology-neutral legislation. The Data Inspection Board is responsible for the supervision of the processing of personal data undertaken by the FRA. On 12 March 2009, the Government decided to assign the Data Inspection Board the special task of monitoring activities from a privacy perspective. The Data Inspection Board is assisted by a consultative group consisting of members of the Riksdag (the Swedish Parliament). In December 2010, the Data Inspection Board will report its findings to the Government.

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

As was reported last year, a Commission of inquiry was set up in 2006 and assigned the task of examining the repeal of the monopoly of Apoteket AB (National Co-operation of Swedish Pharmacies) to sell pharmaceuticals and to make it possible for other operators to sell such products. One of the issues that had to be considered was the registration of prescriptions. The ***Act on Pharmacy Data*** came into effect in July 2009 and the monopoly of Apoteket AB was repealed.

The ***EC Directive on the retention of data processed in connection with the provision of public electronic communication*** has still not been transposed into Swedish law and at present there is no information about when the Government will present a Bill to the Riksdag (the Swedish Parliament).

At the end of November 2009, Sweden signed the ***EU telecoms package*** containing rules aimed at strengthening consumers' rights in relation to telephone and Internet operators. It is now up to the Government to submit a Bill on the telecoms package, which will be implemented by spring 2011 at the latest.

In May 2009, a Commission of inquiry submitted a report, ***Protection of personal privacy in working life.*** The Commission proposes a new act with provisions aiming at clarifying and strengthening employee protection. The proposed act only concerns measures implemented by employers and directed at employees. Medical tests and different kinds of surveillance can serve as examples of issues that are dealt with in the proposed act. The proposal has been referred to different stakeholders from the general public for consideration, inter alia, the Data Inspection Board. The Government still has not decided whether or not to present a Bill.

Video surveillance has been the subject of a review of a Commission of inquiry and a report. ***A new video-surveillance Act*** was submitted to the Government in October 2009. Today video surveillance is regulated by two different acts and their field of application depends on what is being video-surveyed. Many of those who wish to use video surveillance find this situation complicated and the main proposal of the Commission is the introduction of a single act regulating all kinds of video surveillance. In this context, it is also proposed that the Data Inspection Board be given central responsibility for the supervision of the application of the new act. The new act is proposed to come into effect in January 2011.

The Government has submitted a Bill proposing ***amendments to the constitutional law***. A new provision is proposed introducing protection against considerable infringement implying supervision or mapping-out of individuals' personal circumstances. The amendments are proposed to enter into force in January 2011.

As was reported last year, there are problems with credit reporting due to the fact that such information is disclosed on the Internet by way of constitutional protection for information and statements (an amendment to the Fundamental Law on Expression introduced in 2003). The amendment has led to the possibility to disclose credit information on websites without having to comply with the strict rules of the ***Credit Information Act,*** which has led to infringements of privacy and many complaints. The Data Inspection Board has, on several occasions, written to the Government about these problems. The Minister for Justice has announced that a Bill will be presented during spring 2010.

In December 2009, the Government assigned a Commission of Inquiry the task of presenting a proposal for a new organisation for ***anti-doping activity***. One of the tasks is to look into the possibilities to establish an independent national anti-doping organisation, the responsibility of which shall be shared by the state and the central organisation of sports. The possibilities to involve other stakeholders, who can cooperate in the anti-doping work, should also be looked into. The Commission will report back to the Government in October 2010.

B. Major case law

The Swedish Supreme Administrative Court's decision on IP addresses.
A case involving the issue of whether IP numbers can be personal data was finally concluded in 2009. A private organisation with the aim of safeguarding copyright interests had used special software in order to trace users on the Internet who were involved in file sharing. In 2005, the Data Inspection Board concluded that the collection and processing of IP numbers in this case constituted processing of personal data. An appeal was lodged against the Board's decision to the County Administrative Court and the Administrative Court of Appeal, which both upheld the Board's view. Following an appeal to the Supreme Administrative Court, this court decided in April 2009 not to allow the appeal. The decision of the Administrative Court of Appeal, therefore, still stands and the Data Inspection Board's view that an IP number can be personal data is still valid.

In last year's report, the Data Inspection Board outlined a case involving ***RFID-techniques ticket systems with smart cards.*** In 2006 and 2008, the Board carried out inspections regarding public companies' new ticket systems with smart cards that leave electronic traces (systems based on RFID-techniques). The Data Inspection Board decided that the personal data recorded when the passengers used their electronic cards may only be stored for 60 days and that they had to be made anonymous after that. One of the transport companies concerned appealed against the decision and argued that the information about travellers was to be regarded as official documents and, therefore, according to the Archives Act, had to be stored in the absence of specific rules on

deletion. The County Administrative Court in January 2009 repealed the Board's decision and remitted the case for a review. Based on the assessment that the Archives Act was applicable, the Data Inspection Board came to the conclusion that there was no obligation to delete or make the information anonymous. The Board, however, has maintained its view that detailed information about how individuals use public transport should not be stored for an indefinite time. In June 2009, the Board, therefore, wrote to the Government and pointed out the need for new legislation in this regard.

Last year, the Data Inspection Board also gave information about ***video surveillance in schools***. The background is that a web questionnaire, launched in 2008, showed that video surveillance in schools had increased by 150% compared to 2005, when a similar investigation had been carried out. The Board then conducted field inspections in seven schools and found that the video surveillance of pupils' school time infringed the Personal Data Act. The inspections also showed that there was a considerable lack of knowledge of data protection legislation and, therefore, the Board issued a checklist to make it easier for schools to decide when video surveillance is permitted. An appeal was lodged against the Board's decisions of October 2008 to the County Administrative Court that had ruled on the case in September 2009. The appeals were rejected and the Board's decisions upheld. However, appeals have been lodged against two of the five decisions to the Administrative Court of Appeal, where they are now pending. During 2009, the Data Inspection Board carried out four new inspections of schools and found that there are still a number of deficiencies as regards the processing and that the schools have insufficient or no knowledge at all of how long personal data about pupils may be retained. There are no procedures in place for the deletion of data that is no longer needed.

C. Major specific issues

The Pirate Bay trial

The trial against the four men behind the popular sharing site "the Pirate Bay" started in the Stockholm District Court in February 2009. In April, the Court announced its verdict. The Pirate Bay's four co-founders were sentenced to one year in prison and a 3,000,000 EUR fine, for which they are jointly and severally liable. Media all over the world followed the trial and commented on the decision. The Guardian wrote: "The consortium of media and music companies behind the prosecution will be crowing over their victory for years. It's a landmark, certainly, but one that raises more questions than it answers." An appeal was lodged against the sentence to Svea hovrätt (the Svea Court of Appeal) where it is now pending.

In the spring of 2009, the Data Inspection Board invited representatives from some of Sweden's biggest ***social networking sites***. The aim was to draw up recommendations on conditions for users as well as the handling of complaints. In November, the result of this cooperation was presented: "***Secure your site – Guidelines for member conditions as regards sites for young people***".

During 2009, the Data Inspection Board handled several cases related to the ***publication of personal data on the Internet***. Three of them dealt with websites where, for instance, names and addresses of people convicted of different ***sex-related crimes*** were published. The Data Inspection Board reported the cases to the police. A complaint was also lodged with the Data Inspection Board about a website where ***individual persons could grade and comment on companies*** and sometimes also individuals. The Data Inspection Board found that the website itself is responsible to a certain extent and that the processing did not comply with the Personal Data Act. The information has now been deleted from the website and the case closed. In August 2009, the police authorities in Skåne in southern Sweden announced that they intended to ***publish photos from surveillance cameras on the Internet*** in order to get help from the general public to identify persons suspected of crime. Since then, photos from investigations regarding, for instance, assault, fraud and theft have been published. The publication has aroused a lot of attention and the Swedish National Police Board asked for the Data Inspection Board's opinion on the publication. The Data Inspection Board answered that this kind of publication ought only be used in exceptional cases and that the prerequisites for publication should be regulated in law. The Board's opinion was, therefore, also sent to the Ministry of Justice.

A new privacy report was produced ***Privacy Year 2009***, which, like last year's report, contains a comprehensive survey of new legislation, proposals, decisions and techniques that affected privacy during the year.

The Nordic Data Protection Commissioners' meeting
The Data Inspection Board in May 2009 hosted the biannual Nordic meeting for the Nordic countries' Commissioners. The meeting took place in Stockholm and gathered participants from Denmark, Finland, Iceland, Norway and Sweden.

The United Kingdom

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

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

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

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

B. Major case Law

Retention of police records
In 2008 the Commissioner served Enforcement Notices on five police forces, ordering them to delete old criminal convictions from the police national computer (PNC).

This action was taken following our investigation into complaints received from five individuals who had been convicted or cautioned by police on one occasion and had not subsequently been convicted of any other offences.

In each case the Commissioner wrote to the relevant police force and asked for the information to be removed from the PNC, or else "stepped down"; i.e. retained on the PNC but on the basis that only police users could access the information. Each police force agreed to step down the information, but not to delete it.

As a result the Commissioner served enforcement notices on the Chief Constables of each of the forces. Each notice required the conviction information about the individual in question to be deleted from the PNC.

The Chief Constables appealed to the Information Tribunal, seeking to set aside the Commissioner's enforcement notices. In other words the Chief Constables were seeking to ensure that they could retain the relevant conviction information on the PNC.

The Tribunal upheld the enforcement notices issued by the Commissioner, and required the Chief Constables to delete the relevant information about these five individuals.

The five Chief Constables were allowed to appeal to the Court of Appeal, which ruled that the police forces did not need to delete the information and that they had not retained the records in breach of the DPA. The judgment can be viewed at:
www.bailii.org/ew/cases/EWCA/Civ/2009/1079.html

We believe the judgment raises important issues, not just for these and the many other individuals about whom very minor and aged conviction details are held, but also about how the DPA is interpreted in practice. It also engages serious questions about the applicability of Article 8 of the European Convention on Human Rights to conviction data held by the police. We have applied to the Supreme Court for leave to appeal and we hope that the application will be successful so that these issues can be examined by the Supreme Court.

C. Major specific issues

January
We launched the Personal Information Promise on European Data Protection Day. The Promise is a clear statement from the leaders of organisations saying that they value the personal information entrusted to them and will put in place the appropriate resources to look after it. By the end of 2009 around 1,000 organisations had signed the Promise.

We found the Home Office in breach of the DPA after a contractor lost an unencrypted memory stick holding sensitive personal data of thousands of individuals in 2008. Details lost included information about individuals serving custodial sentences and those who had been previously convicted of criminal offences.

March
We seized a covert database containing personal data on 3,213 construction industry workers, and issued an Enforcement Notice against the owner of the database, Mr Ian Kerr, trading as The Consulting Association. The data were used by over 40 construction firms to vet

individuals for employment. Ian Kerr was later fined £5,000 plus court costs, and we served Enforcement Notices on 14 construction firms for breaching the DPA. Some firms had paid thousands of pounds to unfairly obtain personal data about construction workers.

We held our second data protection officers' conference in Manchester, attended by around 300 delegates. This event reflected on the increased profile of data protection, following recent data losses, and on sharing ideas and experiences on how to deal with the challenges faced by data protection officers.

April
In 2008 we commissioned RAND Europe to conduct a review of the European Data Protection Directive. The project assessed the strengths and weaknesses of European data protection arrangements and, by inference, the UK's Data Protection Act. The draft of the final report was presented to the conference of European Data Protection Commissioners hosted by the ICO in Edinburgh, in April 2009, and was published in May.

June
We published our Privacy notices code of practice. The code is designed to help organisations draft clear privacy notices and make sure they collect personal information fairly and transparently.

We also welcomed our new Commissioner, Christopher Graham, who joined us following the end of Richard Thomas's term of office.

October
Our notification fee increased from £35 to £500 for some large organisations. The organisations affected are those with a turnover of £25.9 million or more and at least 250 members of staff. The new rate also applies to public bodies with at least 250 members of staff.

November
The Coroners and Justice Bill received Royal Assent and became an Act of Parliament. As a result, we will have power to audit government departments without their consent, by serving them with an Assessment Notice. Our new auditing powers are due to come into effect in April 2010.

We published The guide to data protection, which provides clear guidance on the practical application of the law, and which has been very well received by stakeholders.

December
We launched a public consultation exercise for our draft Personal information online code of practice at our conference held in Manchester on 9 December. The draft code sets out clear, comprehensive recommendations for handling personal data properly and for giving individuals the right degree of choice and control over it. It should help organisations with an online presence to negotiate areas of legal uncertainty by adopting good practice. We aim to publish the finished code around May 2010.

More details of our activities during 2009 can be found in our annual reports for 2008/09 and 2009/10, which are published on our website www.ico.gov.uk

Chapter Three

EUROPEAN UNION AND COMMUNITY ACTIVITIES

3.1. EUROPEAN COMMISSION

Conference[24]: "Personal data - more use, more protection?" 19-20 May 2009.

The European Commission organised a conference on the use and protection of personal data use and protection to look at new challenges to privacy.

How should personal data be protected in a globalised world with increased mobility and in the wake of modern communication and information technologies and new policies? Which data is accessed and exchanged by public authorities and private companies? How well are current rules on international transfers of personal data working in the age of "cloud computing"? What are the expectations of individuals and business and society as a whole? These and other topical questions were addressed by a conference on the use, exchange and protection of personal data in the EU, organised by the European Commission, which took place in Brussels on 19 and 20 May 2009.

Interested individuals, business leaders, consumer associations, academics, data protection supervisors and public authorities from both the EU and third countries were invited to take part. Among the speakers was the Vice-president of the European Commission in charge of Justice, Freedom and Security, Mr Jacques Barrot.

The conference gave various stakeholders the opportunity to express their views and questions on the new challenges for data protection and the need for an effective information management strategy in the EU. The conference was part of the Commission's open consultation on how the fundamental right to protection of personal data can be further developed and effectively respected, in particular in the area of freedom, justice and security.

[24] http://ec.europa.eu/justice_home/news/events/events_2009_en.htm

Workshop on the Economic Benefits of PETs – 12 November 2009[25]

The European Commission has launched a study on the economic benefits of PETs. The Workshop presented the interim report[26] on this study, which was currently being carried out by London Economics. It also gave a broad range of stakeholders the opportunity to share their experience of PETs. We were hoping that participants would provide us with practical examples as to whether PETs work or not, and how their deployment could be beneficial to all of us. This Workshop was designed for PETs stakeholders (developers, deployers, public authorities, users/consumers). In order to create a practical working environment, the Workshop was limited to the participation of only 50 experts.

Public Consultation on the legal framework for the fundamental right to protection of personal data[27]

The consultation on the legal framework for the fundamental right to protection of personal data was open to the public from 09.07.2009 to 31.12.2009. The objective of the consultation was to obtain views on the new challenges for personal data protection in order to maintain an effective and comprehensive legal framework to protect individuals' personal data within the EU. The issues to be addressed were: a) to give views on the new challenges for personal data protection, particularly in light of the new technologies and globalisation, b) to give views on whether the current legal framework meets these challenges and c) what future action would be needed to address the identified challenges. There were 168 responses received for this public consultation from citizens, organisations (registered and not registered) and public authorities.

ePrivacy Directive

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the Directive on privacy

[25] http://ec.europa.eu/justice_home/news/events/events_2009_en.htm

[26] http://ec.europa.eu/justice_home/news/events/workshop_pets_2009/report_en.pdf

[27] http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

and electronic communications, ePrivacy Directive) has been revised in the process of the review of the Telecom regulatory package that comprises five different EU Directives (Framework Directive, Access Directive, Authorisation Directive, Universal Service Directive and the e-Privacy Directive). A new Regulation setting up the European Body of Telecoms Regulators BEREC is part of the Telecom regulatory package.

Privacy and protection of individuals' data will be strengthened by the new rules introducing mandatory notifications for personal data breaches – the first law of its kind in the EU. This means that communications providers will be obliged to inform the authorities and their customers about security breaches affecting their personal data. This will increase the incentives for better protection of personal data by providers of communications networks and services.

In addition, the rules concerning privacy and data protection are strengthened, e.g. on the use of "cookies" and similar devices. Internet users will be better informed about cookies and about what happens to their personal data, and they will find it easier to exercise control over their personal information in practice. Furthermore, internet service providers will also gain the right to protect their business and their customers through legal action against spammers.

The revised ePrivacy Directive has to be transposed into national laws by May 2011.

3.2. EUROPEAN COURT OF JUSTICE

Order of the Court (Eighth Chamber) of 19 February 2009 (reference for a preliminary ruling from the Oberster Gerichtshof (Austria)) - LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH) (Case C-557/07)[28]

Operative part of the order:
Community law, in particular Article 8(3) of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, read in conjunction with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) does not preclude Member States from laying down an obligation to disclose to private third parties personal data relating to Internet traffic to enable them to initiate civil proceedings for copyright infringements. However, Community law requires that Member States, when transposing Directives 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, 2002/58 and 2004/48, ensure that they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

An access provider, who merely provides a user with Internet access without offering other services such as, inter alia, email, FTP or file sharing services or exercising any control, either in law or in fact, over the services that the user makes use of, must be considered 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29.

Judgment of the Court (Third Chamber) of 7 May 2009 – (reference for a preliminary ruling from the Raad van State (Netherlands)) – College van burgemeester en wethouders

[28] OJ C 113 of 16.05.2009, p.14.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:113:0014:0014:EN:PDF

van Rotterdam v M.E.E. Rijkeboer Netherlands (Case C-553/07)[29]

Operative part of the judgment:
Article 12(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data requires Member States to ensure a right of access to information on the recipients or categories of recipients of personal data and on the content of the data disclosed, not only in respect of the present but also in respect of the past. It is up to Member States to fix a time limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, particularly by way of his rights to object and to bring legal proceedings and, on the other, the burden that the obligation to store that information represents for the controller.

Rules limiting the storage of information on the recipients or categories of recipients of personal data and on the content of the disclosed data to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the necessary determinations.

3.3. EUROPEAN DATA PROTECTION SUPERVISOR

Introduction

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

The main activities of the EDPS, as laid down in Regulation (EC) No 45/2001[30] ("the Regulation"), are to:

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

Supervision

The supervisory tasks range from advising and supporting data protection officers, through prior checking of high-risk data processing operations, to conducting inquiries, including on-the-spot inspections, and handling complaints. Further advice to the EU administration can also take the form of consultations on administrative measures or the publication of thematic guidelines.

All EU institutions and bodies must have at least one data protection officer. In 2009, the total number of **data protection officers** rose to 45. Regular interaction with them and their network is an important condition for effective supervision.

Prior checking of high-risk processing operations continued to be the main aspect of supervision during 2009. The EDPS adopted 110 prior-check opinions on health data, staff evaluation, recruitment, time management, telephone recording, performance tools and security investigations. These opinions are published on the EDPS website and their implementation is followed up systematically.

The implementation of the Regulation by institutions and bodies is also **monitored systematically** by regular stock taking of performance indicators, involving all EU institutions and bodies. Following the spring 2009

[29] OJ C 153 of 04.07.2009, p.10
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:153:0010:0010:EN:PDF

[30] Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p.1.

exercise, the EDPS published a report showing that EU institutions have made good progress on meeting data protection requirements, but a lower level of compliance is observed in most of the agencies.

The EDPS has also carried out four on-the-spot **inspections** in various institutions and bodies. These inspections are followed up systematically and will be undertaken more frequently in the near future. In July 2009, the EDPS adopted an inspection procedure manual and published the key elements of this procedure on its website.

In 2009, the total number of **complaints** received rose to 111, but only 42 of these were found admissible. Many inadmissible complaints involved issues at a national level for which the EDPS is not competent. Most issues in admissible complaints involved alleged violations of confidentiality, excessive collection of data, or illegal use of data by the controller. In eight cases, the EDPS concluded that data protection rules had been breached.

Further work was also done in consultation on **administrative measures** envisaged by EU institutions and bodies in relation to the processing of personal data. A variety of issues was raised, including transfers of data to third countries or international organisations, processing of data in case of a pandemic procedure, data protection in the Internal Audit Service, and implementing rules of Regulation (EC) No 45/2001.

The EDPS adopted **guidelines** on the processing of personal data for recruitment and on health data in the workplace. In 2009, the EDPS also held a public consultation on video-surveillance guidelines, among others emphasising "Privacy by Design" and accountability as key principles in this context.

Consultation

A number of significant events helped bring the prospect of a new **legal framework for data protection** closer. Achieving this prospect will be a dominant subject on the EDPS agenda in the coming years.

At the end of 2008, a general legal framework for data protection in the area of police and judicial cooperation was adopted at EU level. Although not fully satisfactory, it was an important step in the right direction.

In 2009, a second major development was the adoption of the revised e-Privacy Directive as part of a larger package. This was also a first step in the modernisation of the legal framework for data protection.

The entry into force of the Lisbon Treaty on 1 December 2009 not only resulted in the Charter of Fundamental Rights becoming binding on institutions and bodies, as well as on Member States when acting in the scope of EU law, but also in the introduction of a general basis for a comprehensive legal framework in Article 16 TFEU.

In 2009, the Commission also launched a public consultation on the future of the legal framework for data protection. The EDPS has worked closely with colleagues in order to ensure an adequate joint input to this consultation and has used various occasions to highlight the need for more comprehensive and more effective data protection in the European Union.

The EDPS has continued to implement its general **consultation policy** and issued a record number of legislative opinions on different subjects. This policy also provides for a pro-active approach, involving a regular inventory of legislative proposals to be submitted for consultation, and availability for informal comments in the preparatory stages of legislative proposals. Most EDPS opinions were followed up in discussions with Parliament and Council.

In 2009, the EDPS followed the developments concerning the **Stockholm Programme** and its vision for the next five years in the area of justice and home affairs with particular interest. The EDPS advised on the development of the programme and took part in the preparatory work for the European Information Model.

Other work in this area related to the review of the Eurodac and Dublin Regulations, the setting up of an Agency for the operational management of large-scale IT systems, and a coherent approach to supervision in this field.

In the context of **e-Privacy and technology**, apart from the general review mentioned above, the EDPS was involved in issues relating to the Data Retention Directive, the use of RFID tags or intelligent transport systems, and the RISEPTIS report on "Trust in the Information Society".

In the context of **globalisation**, the EDPS was involved in the development of global standards, the transatlantic dialogue on data protection and law enforcement data, as well as in issues on restrictive measures relating to suspected terrorists and certain third countries.

Other areas of substantial EDPS interest have been **public health** – including cross-border healthcare, e-health and pharmaceuticals monitoring – and **public access to documents** – such as the revision of public access Regulation (EC) 1049/2001 and various court cases about the relationship between public access and data protection.

Cooperation

The main platform for cooperation between data protection authorities in Europe is the **Article 29 Working Party**. The EDPS takes part in the activities of the Working Party, which plays an important role in the uniform application of the Data Protection Directive.

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

Special mention should be made of the joint contribution on the "Future of Privacy" in reply to the consultation of the European Commission on the EU legal framework for data protection, and the consultation of the Commission on the impact of "body scanners" in the field of aviation security.

One of the most important cooperative tasks of the EDPS involves **Eurodac** where the responsibilities for supervision are shared with national data protection authorities. The Eurodac Supervision Coordination Group – composed of national data protection authorities and the EDPS – met three times and concentrated on the implementation of the work programme adopted in December 2007.

One of the main results was the adoption in June 2009 of a second inspection report focusing on two issues: the right to information for asylum seekers and the methods for assessing the age of young asylum seekers.

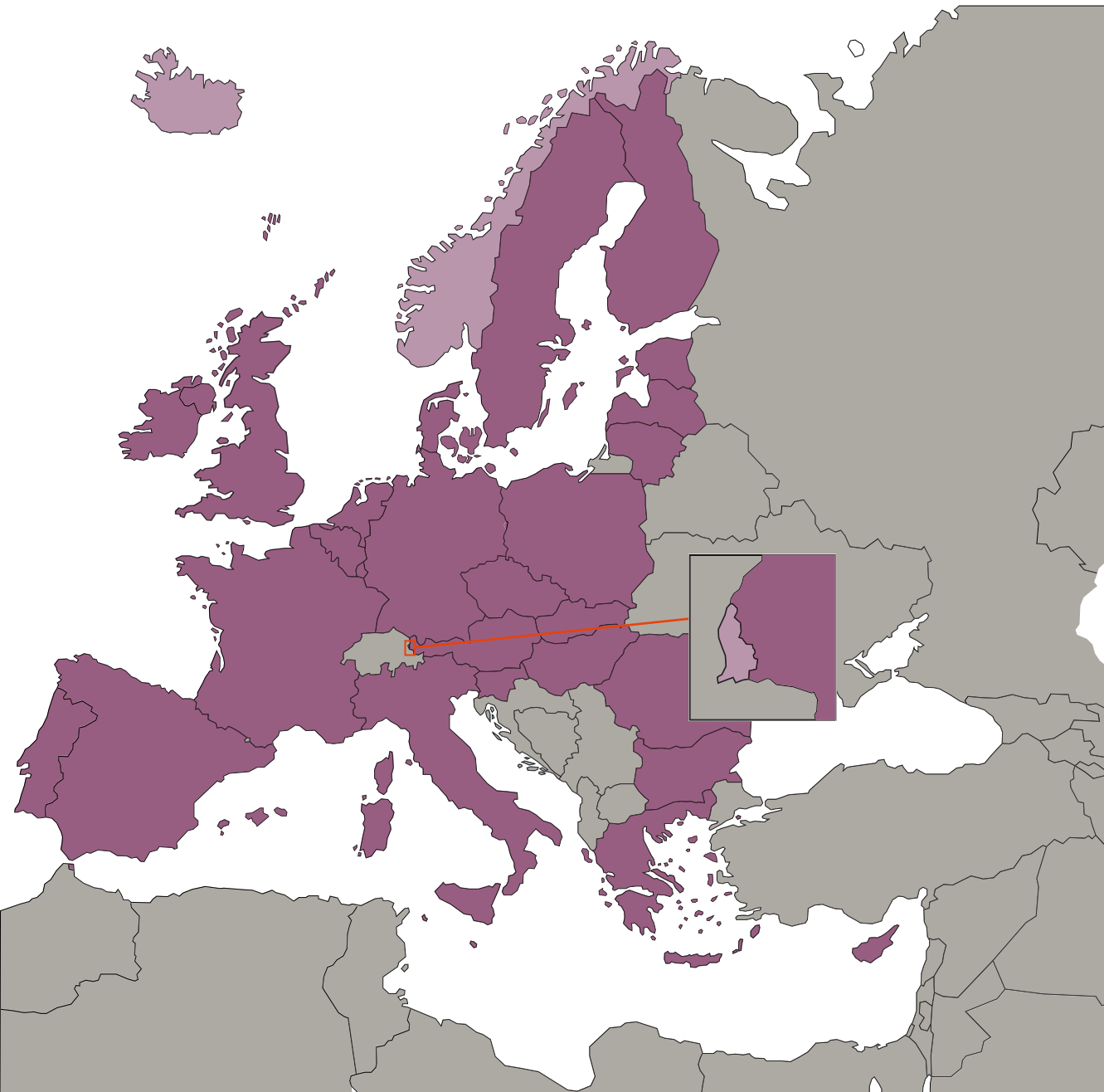
The EDPS continued its close cooperation with data protection authorities in the former "third pillar" – the area of **police and judicial cooperation** – and with the Working Party on Police and Justice. In 2009, this cooperation included contributing to the debate on the Stockholm Programme and evaluating the impact of the Council Framework Decision on data protection.

Cooperation in other **international forums** continued to attract attention, especially the 31st International Conference of Data Protection and Privacy Commissioners in Madrid, which led to a set of global standards for data protection.

The EDPS also organised a workshop on "Responding to security breaches" in the context of the "London initiative" launched at the 28th International Conference in November 2006 to raise awareness of data protection and to make it more effective.

Chapter Four

PRINCIPAL DEVELOPMENTS IN EEA COUNTRIES



Iceland

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

In 2009, a number of legal acts and administrative rules concerning or having an effect on data protection were passed regarding Directive 95/46/EC (but none, however, regarding Directive 2002/58/EC). These are the most important ones:

1. Act No. 37/2009, amending the Act on Unemployment Insurance, No. 54/2006. – By means of Act No. 37/2009, the Labour Directorate's authority to collect data was increased. The Labour Directorate did have the authority to collect data, which was necessary to implement Act No. 54/2006, from tax authorities, the social and medical insurance authorities, the Child Support Collection Centre, and pension funds. By means of Act No. 37/2009, the Labour Directorate was also given the authority to collect data from schools of upper secondary and university level. In this respect, the Labour Directorate obtained lists of those studying in those schools, since registration at a school can affect the right to receive unemployment benefits.

2. Act. No. 48/2009, amending the Act on Biobanks, No. 110/2000. – The Act on Biobanks contains provisions on the protection of personal data with regard to the collection, storage and use of biological samples. Originally, all biosamples were to be kept separate from personal identification markers. Act No. 48/2009 changed this. Now, a distinction is made between research samples and clinical samples. The former shall be kept without personal identification, and the connection between samples and personal identification shall be in keeping with rules from the DPA (currently Rule No. 918/2001). The latter samples, however, may be marked with personal identification markers, but shall be stored in such a way that they are not lost or damaged, and are not accessible to unauthorised people. The purpose of Act No. 48/2009 was to eliminate the danger of mistaken identification of clinical samples, which might put the security of patients at risk.

3. The Health Records Act, No. 55/2009. – This Act lays down the obligation to keep health records. The Act states that its purpose is to introduce rules on health records, so that patients can be provided with the best possible health service at any time, while also ensuring protection of health data. Health records shall be entered in electronic form as far as possible. The Act allows health institutions and self-employed healthcare practitioners to connect their health information systems containing patients' health records, or to operate a joint health information system. Patients have the right to prohibit the sharing of data on them in connected health information systems. Furthermore, patients can prohibit access to their data in a joint health information system, in whole or in part, outside the healthcare facility or premises of a healthcare practitioner where the records are entered. Patients can decide, when receiving treatment, that health records with respect to the treatment shall not be accessible to others except for the person making the entry, the supervisor of the health records, and, as applicable, other specified healthcare practitioners. Should it be deemed necessary, with respect to treatment, for other healthcare practitioners to have access to the health data in question, the patient shall be informed of this, and also that any refusal to authorise necessary access to the health records may be equivalent, under some circumstances, to refusal of treatment. Compliance with the provisions of the Act shall, in the first instance, be monitored by those responsible for health information systems, and in the second instance by the Medical Director of Health and the DPA. Should monitoring reveal a real likelihood that the personal privacy rights of a patient have been violated, the offence shall be reported to the police.

4. Act No. 146/2009, amending the Act on an Investigation of the Events Leading to and the Causes of the Downfall of the Icelandic Banks in 2008, and Related Events, No. 142/2008. – Act No. 146/2009 inserts clauses on the procedure to be followed by the Icelandic Parliament (Althing) when reacting to the report of the Special Investigative Commission, appointed by the Althing according to Act No. 142/2008. The Act contains provisions

on the databases that have been created in the course of the Commission's Activities. These databases contain extensive data on individuals. Some of this data has been published in the Commission's report issued in April 2010 (mostly data concerning businessmen, politicians, and senior officials), since the data was considered to shed light on the downfall of the Icelandic banks. However, the bulk of the data is not considered to be of such value that their publication is necessary. Act No. 146/2009, therefore, includes provisions granting protection for this data so that it is not made available to those who do not have legitimate grounds to access it. According to the Act, access for research purposes can be viewed as legitimate. However, processing for research purposes shall not entail the publication of personally identifiable data.

B. Major case law

None to report.

C. Major specific issues

One of the foremost issues regarding data protection in the year 2009 was a research project conducted by the National Bank of Iceland, in which extensive data on individuals' financial matters from many parties, such as banks and other financial institutions, the Labour Directorate, pension funds, and the Social Insurance Administration, was linked. The purpose of linking this data was to gain insight into how the financial crisis in Iceland affects individuals and families, so as to be better prepared to tackle the crisis. The DPA gave permits for the link with provisions on technical and organisational security measures, including anonymisation. When data was not being processed, the computer on which the data was stored was kept by the DPA. As stipulated in the permits, the hard drive of the computer containing all the data was destroyed in early 2010.

On 28 April, the DPA issued a decision regarding the use of data in the Central Drugs Prescriptions Database in Iceland, which has been operated by the Directorate of Health according to law since 2003. The law, i.e. Article 27 of the Drugs Prescription Act, No. 93/1994, as amended by Act No. 89/2003, states for which uses the database may be utilised, i.e. mainly for administrative purposes, including the investigation of alleged misuse of habit-forming drugs. One individual had asked for a prescription for such a drug. The doctor whom the individual attended asked the Directorate of Health about the individual's drug use and received answers stating that the individual had a history of misuse of habit-forming drugs. The individual was not informed of this use of data in the database until afterwards and complained to the DPA. In the aforementioned decision, the DPA came to the conclusion that the transmission of the information on the complainant did not conform to Article 27 of the Drugs Prescription Act and that the Directorate of Health had, therefore, not acted lawfully when giving said information to the doctor.

On 16 December 2009, the DPA issued a decision on the processing of data in IP addresses conducted by the Labour Directorate. Those who wish to receive unemployment benefits send an electronic notice each month to the Directorate confirming that they are unemployed. According to the Directorate's interpretation of the legislation on unemployment, those who are unemployed must stay in Iceland if they are to be entitled to receive benefits, i.e. so as to be ready to be employed at short notice. The IP address in an electronic notice sent to the Directorate contained information revealing that the individual in question was not in Iceland. The Directorate sent a letter to this individual stating that it had information on the individual's stay outside Iceland, but did not specify how it had come across this information. The individual complained to the DPA, which came to the conclusion, in the aforementioned decision, that it would have been right to give information on the website of the Labour Directorate that IP addresses were collected and that data contained in the addresses was processed, among other things, to find out whether an individual was staying outside Iceland.

Liechtenstein

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

One of the tasks of the Data Protection Agency (*Datenschutzstelle* - DSS) is to comment on draft legislation and decrees that are relevant to data protection and to check conformity with the provisions of Directive 95/46/EC. In 2009, the DSS was asked to give an opinion on a total of 34 legislative proposals in various stages of the legislative process. In the framework of the legislative proposals particularly the following points will be examined in greater detail as they affect important legal aspects of data protection:

The last annual report already contained a detailed report on the two partial amendments of the Data Protection Law (DPL: *Datenschutzgesetz* - DSG). The first amendment came into effect as early as 1 January 2009[31] and the other by 1 July 2009[32]. In parallel, the Data Protection Act (*Datenschutzverordnung* - DSV) was adapted, and also came into effect in July[33]. In particular, the DSV created the new institution of a Data Protection Officer in companies or authorities.[34] The function of an internal Data Protection Officer was intended to support and strengthen the individual responsibility of the owners of databases. Furthermore, the creation of the post of a Data Protection Officer is also seen as a competitive advantage for companies. Private persons or authorities who appoint an internal Data Protection Officer are granted particular advantages, such as the exemption from the notification obligation under certain circumstances. Private persons are even exempted from the obligation to draw up processing regulations for automated databases. In order to best exploit the legal advantages, the DSS must be informed of the internally appointed Data Protection Officers, the names of which are published.

In practice, particular attention was given to innovations for the strengthened independence of the DSS[35], for data transfer abroad and for video surveillance. In connection with cross-border data transfer, special mention deserve the newly introduced obligation to obtain approval for individually agreed data protection agreements and for obligatory internal data protection regulations in companies.[36] Insofar as there is no relevant legislation in the foreign country in question guaranteeing appropriate data protection, these agreements must first be approved by the government. The DSS must provide an opinion during the course of the approval procedure. This opinion must state whether the guarantees or individual data protection regulations provide appropriate protection in terms of the DSG of Liechtenstein. When issuing approval, the government is generally bound by the opinion of the DSS.

The introduction of a general legal basis for video surveillance in areas accessible to the public[37] engaged the resources of the DSS during the reporting year considerably. Video surveillance in public areas has been subject to obligatory approval from the DSS since 1 July 2009. Generally, approval must be obtained before the system is put into operation. For already existing surveillance systems, a transitional period was established until the end of the year. For the approval procedure it was necessary to draft online application forms, provide assistance for filling in the forms and detailed guidelines, in advance, and to inform the public accordingly. It should be noted that obligatory approval applies only when it is possible to identify persons with the data obtained, when data is processed and when they are obtained in publicly accessible areas. Conversely, this means that – for example - video recordings for the purely private or family sphere, image transmissions exclusively in real time or recordings of webcams that do not allow identification of people, do not require approval.

A key legislative proposal related to the revision of the Communications Act (*Kommunikationsgesetz* - KomG), which was not finalised during the reporting year:

[31] LGBl. 2008 No. 273.

[32] LGBl. 2009 No. 46.

[33] LGBl. 2009 No. 209.

[34] Art. 4a, 13a, 23 para. 2 DSV.

[35] See in connection with this the detailed report of Liechtenstein in the 12th annual report of the Article 29 Data Protection Working Party, p. 132, and also the Activity Report of the Data Protection Officers of the Principality of Liechtenstein, 2008, 10.1.

[36] Art. 8 para. 3 DSG in connection with art. 6 DSV.

[37] Art. 6a DSG in connection with art. 27 DSV.

As early as 2006, Liechtenstein had introduced the retention of traffic data into the KomG, although the Directive 2006/24/EC is not yet part of the EEA Agreement and, therefore, there no implementation obligation exists. These regulations were the object of repeated criticism. The retention of traffic data for a period of six months – in conformity with the Article 29 Data Protection Working Party – was seen as constituting a major interference into citizens' rights to freedom and their private life. The government has taken these criticisms as an opportunity to revise the regulations in question in view of a more citizens and fundamental rights friendly arrangement. It is also intended to regulate strict conditions for access to and/or evaluation of retained data.[38] Furthermore, global control of data protection and data security is provided by the DSS.

B. Major case Law

Nothing significant.

C. Major specific issues

The intensive work that had already begun in the previous year in preparation of the accession of Liechtenstein to the Schengen and Dublin agreements was continued and intensified[39]. Thus, the DSS had to deal already with the legal instruments on the further development of the Schengen acquis, such as the implementation of the so-called Swedish Initiative (Framework Decision 2006/960/JI). The findings of other Schengen States were able to be used to prepare the data protection evaluation. During the reporting year a test evaluation was conducted in the area of data protection, yielding positive experiences. The main emphasis was placed on the independence and structure of the Data Protection Agency, its legal duties and competences of investigation, as well as on the rights of citizens. At the centre of the preparations were the answers to a questionnaire in which the framework conditions with regard to "Schengen maturity" are to be set forth, as well as the drafting of documentation.

Although Liechtenstein has no access to the data yet, their participation as observers at sessions of the various commissions and the joint Schengen Control Body yielded them valuable information concerning the way in which Schengen functions and works.

Furthermore, the central tasks of the Data Protection Agency also include informing and sensitising the public on data protection. The DSS internet page is most frequently used to inform the public. The Newsletter also contributes considerably to informing the public. This publication provides a monthly report on a topical subject.

On its internet page, the Data Protection Agency conducted an online survey during the reporting year for the first time. Altogether, four groups of questions on the subject of data protection were asked, covering the following areas: General – Information – Trust – Behaviour. The media witnessed considerable interest in the results of this survey, one of which was that the majority of participants felt they were insufficiently informed about their data protection rights. Internet and data protection was a subject on which participants wanted more information. This was taken up, and a training course for employees of the Liechtenstein Territorial Administration was organised.

On European Data Protection Day on 28 January, the DSS along with the Institute for Economic IT of Liechtenstein College extended an open invitation to a public event entitled: "Because they don't know what they are doing?! – Social networks under the magnifying glass".[40] The objective of the event was to draw attention to the subject of data protection and to sensitise the public.

In order to resolve certain legal questions, the Data Protection Agency commissioned two legal opinions: these concerned exceptions to doctors' obligations to confidentiality and the tension between professional secrecy and professional assistance with special emphasis on the methods of interpretation known as *lex specialis* and *lex posterior*. The latter legal opinion contains important lessons that are still to be assessed.

[38] Report and proposal no. 110/2009, p. 113.

[39] Cf. Activity report 2008, 10.1.

[40] http://www.llv.li/amtsstellen/llv-dss-datenschutztag/llv-dss-datenschutztag-archiv.htm.

Norway

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

On 9 January, the Storting (Norwegian Parliament) adopted a change in the Personal Data Act. Section 26 was replaced by a new act regulating direct marketing empowering the Consumer Ombudsman to act in the public's interest whenever the public was exposed to unlawful and unethical marketing. The former section 26 assigned this power to the Data Inspectorate.

In early 2009, an agreement between the Inspectorate and the National Collection Agency was finalised, enabling the Inspectorate to collect issued fines and to issue fines in the future.

As mentioned in the last annual report, the Storting adopted the new health research act. The act came into force on 1 June 2009. The Data Inspectorate is no longer competent to grant permission to health research projects. Nevertheless, the Data Inspectorate still has the power to conduct audits on data controllers to make sure they comply with the Health Research Act.

The Personal Data Regulations gained a new chapter 9 regulating the "Examination of e-mail inboxes, etc." The regulation was a codification of the official practice of the Norwegian Data Inspectorate in these matters. The most important issue is that employers must follow specific protocol to look into employees personal e-mail inboxes and personal space in computer networks. The regulation states clearly that there must be some part of the employees' "space in the business" that is protected from surveillance and logging.

The Personal Data Act is to be revised and the Data Inspectorate has suggested some minor changes aiming to bring the act into line with technological development as well as developments in society.

B. Major case law

None to report.

C. Major specific issues

Data Retention Directive

2009 was dominated by the debate on the Data Retention Directive. The Data Inspectorate stressed that the directive represents a break with the current tradition of registration and storage of communications data. In our view, the directive is contrary to central legal principles, freedoms and human rights. An implementation of the directive in Norwegian law means that large amounts of data about Norwegian citizens' communications and movements will be recorded and stored for a long period of time. One of the key political questions is whether the Parliament should use our reservation rights in the EEA Agreement.

In the debate on the Directive, followers claim that privacy will not be affected by the data storage because there will be clear and strict conditions for use of the information. The consultation draft on the Norwegian implementation of the directive points out that the information will not be looked at by police unless there is concrete suspicion, and that a court has approved such access.

Privacy Protection in Western legal tradition should not only defend against subsequent use of collected information, but also against the vast collection of personal information. A systematic storage of information just in case they become necessary in a later investigation may challenge the presumption of innocence, which is an important principle in the Norwegian legal system.

Serious findings in the Cancer Registry

In a meeting between the Cancer Registry and the Norwegian Data Inspectorate in autumn 2008, it emerged that the Cancer Registry themselves doubted whether the recording of information on healthy women who have participated in a mammography programme had a legal basis.

The Data Inspectorate reviewed the matter and found that since 2002 the Cancer Registry has processed information on approximately 600,000 women without the consent of the women in line with cancer registry regulatory requirements.

Proposal on establishing a national registry of heart and vascular diseases

The Department of Health proposed establishing a central registry for heart and vascular diseases. The register is proposed to contain directly identifiable and mandatory information. This means that the registry will include directly identifiable information, not based on consent from each patient, with no possibility to "opt out" of being registered.

The mentioned register is just one of several central research databases, and will form a "template" for similar records for other disease groups. The Data Inspectorate, therefore, emphasises the importance of carefully thinking about the legal basis for the establishment of such registers. The Inspectorate highlights that the main legal basis for registration should be consent, especially when the information in the registry will be directly identifiable. Tables that are not based on consent must, therefore, be based on pseudonyms, or otherwise be subject to special protection.

Proposals for new exemptions from the health personnel's duty of confidentiality

The Department of Health has in the message year proposed a new provision in the Health Personnel Act section 29 b to provide an exemption from client/patient confidentiality for the purpose of quality assurance, administration, planning or management of health services.

The Data Inspectorate is concerned about the ever new statutory exemptions applicable to health personnel's confidentiality. The Department's proposal will provide a very broad mandate, which in time may significantly undermine health personnel confidentiality. This means that patients are in danger of losing control over their health information.

Audit - electronic ticketing

In the spring of 2009, the Data Inspectorate conducted three audits on public transport providers. The central theme of the inspections was the processing of personal data in connection with electronic ticketing - that is, electronic travel cards.

It is important for the public, in the future, to be able to travel freely in society without having to leave electronic traces of where they have been, and when the trip took place. The Authority's assessment is a prerequisite for real freedom of movement and protection of privacy.

It is important to travellers that they be able to use ordinary public transport systems without information being recorded about their movements. In the case of personal electronic tickets, a key point was that the transport provider collected and stored more information than strictly necessary. The Data Inspectorate has required the companies to delete travel-identifiable information immediately after or a short time after the trip is paid for.

Chapter Five

MEMBERS AND OBSERVERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY

MEMBERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2009

Austria	**Belgium**
Mrs Waltraut Kotschy Austrian Data Protection Commission (Datenschutzkommission) Hohenstaufengasse 31 - AT - 1014 Wien Tel: +43 1 531 15 / 2525 Fax: +43 1 531 15 / 2690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Mr Willem Debeuckelaere Commission for the protection of privacy (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute, 139 - BE - 1000 Bruxelles Tel: +32(0)2/213.85.40 Fax: +32(0)2/213.85.65 E-mail: commission@privacycommission.be Website: http://www.privacycommission.be/
Bulgaria	**Cyprus**
Mr Krassimir Dimitrov Commission for Personal Data Protection –CPDP (Комисия за защита на личните данни) 15, Acad.Ivan Evstratiev Geshov blvd. BG- 1431 Sofia Tel+359 2 915 3501 Fax: +359 2 915 3525 E-mail: kzld@government.bg kzld@cpdp.bg Website: http://www.cdpd.bg	Mrs Goulla Frangou Commissioner for Personal Data Protection (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2nd floor - CY - 1082 Nicosia (P.O. Box 23378 - CY - 1682 Nicosia) Tel: +357 22 818 456 Fax: +357 22 304 565 E-mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy
Czech Republic	**Denmark**
Mr Igor Nemec Office for Personal Data Protection (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tel: +420 234 665 111 Fax: +420 234 665 501 E-mail: posta@uoou.cz Website: http://www.uoou.cz/	Mrs Janni Christoffersen Danish Data Protection Agency (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tel: +45 3319 3200 Fax: +45 3319 3218 E-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk

Estonia	**Finland**
Mr Viljar Peep Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) Väike - Ameerika 19 - EE - 10129 Tallinn Tel: +372 6274 135 Fax: +372 6274 137 E-mail: info@aki.ee Website: http://www.aki.ee	Mr Reijo Aarnio Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki (P.O. Box 315) Tel: +358 10 36 166700 Fax: +358 10 36 166735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi
France	**Germany**
Mr Alex Türk Chairman President of the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés - CNIL) Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 Mr Georges de La Loyère French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés - CNIL) Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-mail: laloyere@cnil.fr Website: http://www.cnil.fr	Mr Peter Schaar The Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) Husarenstraße 30 - DE -53117 Bonn Tel: +49 (0) 228 99-7799-0 Fax: +49 (0) 228 99-7799-550 E-mail: poststelle@bfdi.bund.de Website: http://www.bfdi.bund.de Mr. Alexander Dix (representing the German States / Bundesländer) The Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit) An der Urania 4-10 – DE – 10787 Berlin Tel: +49 30 13 889 0 Fax: +49 30 215 50 50 E-mail: mailbox@datenschutz-berlin.de Website: http://www.datenschutz-berlin.de
Greece	**Hungary**
Mr Christos Yeraris Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 –Athens - Greece Tel: +30 210 6475608 Fax: +30 210 6475789 E-mail: christosyeraris@dpa.gr Website: http://www.dpa.gr	Mr András Jóri Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary (Adatvédelmi Biztos) Nador u. 22 - HU - 1051 Budapest Tel: +36 1 475 7186 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Website: www.adatvedelmibiztos.hu

Ireland	**Italy**
Mr Billy Hawkes Data Protection Commissioner (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE -Co.Laois Tel: +353 57 868 4800 Fax:+353 57 868 4757 E-mail: info@dataprotection.ie Website: http://www.dataprotection.ie	Mr Francesco Pizzetti Italian Data Protection Authority (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Roma Tel: +39 06.69677.1 Fax: +39 06.69677.785 E-mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Website: http://www.garanteprivacy.it
Latvia	**Lithuania**
Mrs Signe Plumina Data State Inspectorate (Datu valsts inspekcija) Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia Tel: +371 6722 31 31 Fax: +371 6722 35 56 E-mail: signe.plumina@dvi.gov.lv, info@dvi.gov.lv Website: http://www.dvi.gov.lv	Mr Algirdas Kunčinas State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) A.Juozapaviciaus str. 6 / Slucko str. 2, LT-01102 Vilnius Tel: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-mail: ada@ada.lt Website: http://www.ada.lt
Luxembourg	**Malta**
Mr Gérard Lommel National Commission for Data Protection (Commission nationale pour la Protection des Données - CNPD) 41, avenue de la Gare - L - 1611 Luxembourg Tel: +352 26 10 60 -1 Fax: +352 26 10 60 – 29 E-mail: info@cnpd.lu Website: http://www.cnpd.lu	Mr Joseph Ebejer Data Protection Commissioner Office of the Data Protection Commissioner 2, Airways House High Street Sliema SLM 1549 MALTA Tel: +356 2328 7100 Fax: +356 23287198 E-mail: joseph.ebejer@gov.mt Website: http://www.dataprotection.gov.mt

The Netherlands	**Poland**
Mr Jacob Kohnstamm Dutch Data Protection Authority (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ The Hague Tel: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl	Mr Michał Serzycki Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw Tel: +48 22 860 70 86 Fax: +48 22 860 70 90 E-mail: Sekretariat@giodo.gov.pl Website: http://www.giodo.gov.pl
Portugal	**Romania**
Mr Luís Novais Lingnau da Silveira National Commission of Data Protection (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lisboa Tel: +351 21 392 84 00 Fax: +351 21 397 68 32 E-mail: geral@cnpd.pt Website: http://www.cnpd.pt	Mrs Georgeta Basarabescu National Supervisory Authority for Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, RO - Bucharest Tel: +40 21 252 5599 Fax: +40 21 252 5757 E-mail: georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Website: www.dataprotection.ro
Slovakia	**Slovenia**
Mr Gyula Veszelei Office for the Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky) Odborárske námestie 3 - SK - 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441 E-mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	Mrs Natasa Pirc Musar Information Commissioner (Informacijski pooblaščenec) Vošnjakova 1, SI - 1000 Ljubljana Tel: +386 1 230 97 30 Fax: +386 1 230 97 78 E-mail: gp.ip@ip-rs.si Website: http://www.ip-rs.si

Spain	**Sweden**
Mr Artemi Rallo Lombarte Spanish Data Protection Agency (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES - 28001 Madrid Tel: +34 91 399 6219/20 Fax: + +34 91 445 56 99 E-mail: director@agpd.es Website: http://www.agpd.es	Mr Göran Gräslund Data Inspection Board (Datainspektionen) Fleminggatan, 14 (Box 8114) - SE - 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
United Kingdom	**European Data Protection Supervisor**
Mr Christopher Graham Information Commissioner's Office Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel: +44 1625 545700 Fax: +44 1625 524510 E-mail: please use the online enquiry form on our website Website: http://www.ico.gov.uk	Mr Peter Hustinx European Data Protection Supervisor - EDPS Postal address: 60, rue Wiertz, BE - 1047 Brussels Office: rue Montoyer, 63, BE - 1047 Brussels Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

OBSERVERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2009

Iceland	**Norway**
Mrs Sigrun Johannesdottir Data Protection Authority (Persónuvernd) Raudararstigur 10 - IS - 105 Reykjavik Tel: +354 510 9600 Fax: +354 510 9606 E-mail: postur@personuvernd.is Website: http://www.personuvernd.is	Mr Georg Apenes Data Inspectorate (Datatilsynet) P.O.Box 8177 Dep - NO - 0034 Oslo Tel: +47 22 396900 Fax: +47 22 422350 E-mail: postkasse@datatilsynet.no Website: http://www.datatilsynet.no
Liechtenstein	**Republic of Croatia**
Mr Philipp Mittelberger Data Protection Commissioner Data Protection Office (Datenschutzstelle, DSS) Kirchstrasse 8, Postfach 684 – FL -9490 Vaduz Tel: +423 236 6090 Fax: +423 236 6099 E-mail: info@dss.llv.li Website: http://www.dss.llv.li	Mr. Franjo Lacko Director Mrs Sanja Vuk Head of department for EU and Legal Affairs Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka - AZOP) Republike Austrije 25, 10000 Zagreb Tel: +385 1 4609 000 Fax: +385 1 4609 099 e-mail: azop@azop.hr or info@azop.hr website: http://www.azop.hr/default.asp
the former Yugoslav Republic of Macedonia	
Mrs. Marijana Marusic Directorate for Personal Data Protection (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tel: +389 2 3244 760 Fax: +389 2 3244 766 Website: www.dzlp.mk, info@dzlp.gov.mk	

Secretariat of the Article 29 Working Party

Mrs. Marie-Hélène Boulanger
Head of unit
European Commission
Directorate-General for Justice
Data Protection Unit
Office: LX46 01/190 - BE - 1049 Brussels
Tel: +32 2 295 12 87
Fax: +32 2 299 8094
E-mail: Marie-Helene.Boulanger@ec.europa.eu
Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

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

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

DS-AA-11-001-EN-C doi:10.2838/38069

ISBN 978-92-79-19984-4