41AS78_pages_limi_EN 21-01-2005 11:26 Pagina 1

European Commission

Seventh 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 years 2002 and 2003

adopted on 21 June 2004

41AS78_pages_limi_EN 21-01-2005 11:26 Pagina 2

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number:
00 800 6 7 8 9 10 11

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server (http://europa.eu.int).

Cataloguing data can be found at the end of this publication.

Luxembourg: Office for Official Publications of the European Communities, 2004

ISBN 92-894-6638-3

© European Communities, 2004
Reproduction is authorised provided the source is acknowledged.

Printed in Belgium

PRINTED ON WHITE CHLORINE-FREE PAPER

CONTENTS

* Asterisks denote documents adopted in 2003.

FOREWORD
BY MR STEFANO RODOTÀ, CHAIRMAN OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY

This report on the activity of the Article 29 Data Protection Working Party covers the years 2002 and 2003. It was a period of key importance in terms of drawing a balance of the activity carried out to implement Directive 95/46/EC as well as of starting work on the electronic communications directive (2002/58/EC), especially with regard to the implementation of the new opt-in principle. A wide range of issues were addressed: from contractual clauses to new technologies, from the fight against terrorism to video surveillance. The Working Party came to play an important role within the framework of the unrelenting constitutionalisation of the right to personal data protection.

This right had already been set out as a new autonomous right in the Charter of Fundamental Rights of the European Union; it was subsequently reaffirmed not only by the Draft Constitution for Europe, but by the recent case-law of the Court of Justice of the European Communities — which was seized for the first time with cases concerning the scope of this fundamental right. Additionally, both Article 8 of the Charter and Article 50 of the Draft Constitution expressly require that compliance with the relevant provisions be supervised by independent authorities.

Acknowledging the important mission with which it has been entrusted, the Working Party dealt with the issues related to citizens' fundamental rights in respect of the new technological scenarios; however, it did not fail to get back to issues already addressed in the past in order to draw a balance and develop new guidelines based on the experience gathered. This is the perspective in which one should also see the Working Party's opening-up to public consultation — for instance, concerning the safeguards applying to the use of video surveillance, the feasibility of binding contractual rules, and the viability of the code of conduct submitted by European direct marketers. This approach enhanced the Working Party's transparency through the increased involvement of civil society.

Furthermore, the experience of these two years has testified to the Working Party's rising visibility as well as to its having come to play the role of important authoritative participant in discussions held at the highest institutional levels. In particular, the European Parliament has always paid the utmost attention to the stance taken by the Working Party on sensitive issues such as traffic data retention and transborder data flows. This is shown, *inter alia*, by the reference made expressly to Working Party documents in the resolutions adopted by both the Committee on Freedoms and Citizens' Rights and Parliament itself.

A non-exhaustive, though significant, list of the issues addressed by the Working Party is as follows:

- video surveillance;
- standard contractual clauses;
- binding corporate rules;
- biometrics;
- e-government;
- FEDMA code of conduct;
- reuse of public data;
- online authentication services;
- surveillance of electronic communications in the workplace;
- Whois.

In the past two years, the Working Party was also called upon to tackle highly complex problems featuring unprecedented issues. An example is provided by the work done on transfer to third countries of passengers' PNR data. The Working Party devoted much energy to this topic and reaffirmed that a balanced approach to the fight against terrorism should not result in disproportionate unjustified restrictions on the data protection principles set out in Directive 95/46/EC. In particular, the request from US customs authorities to directly access a wide range of data concerning all passengers on flights between Europe and United States, and retain these data for a long period with a view to purposes going beyond the fight against terrorism in the absence of suitable legal and institutional safeguards for passengers, was the subject of continued attention by the Working Party. The desirability of different solutions affording a greater measure of respect for the fundamental right to data protection was repeatedly highlighted by the Working Party.

The past year was also extremely important on account of the presentation by the European Commission of the first report on the implementation of Directive 95/46/EC. The report drawn up five years after entry into force of the directive pointed out the basic soundness and validity of its framework; however, it also stressed that there were sectors in need of improved implementation. The Working Party set to work immediately on the basis of these guidelines and decided to address some of the most important issues as part of its current work programme by setting up ad hoc working groups.

INTRODUCTION

This is the seventh report covering the years 2002 and 2003 of the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter 'the Working Party' or 'the Article 29 Working Party'. The Working Party is the independent European Union advisory body on data protection and privacy set up by Article 29 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 (data protection directive) and composed of the national supervisory authorities. The Working Party draws up an annual report which is intended to give an overview of the situation of the protection of individuals concerning the processing of personal data in the European Union and in third countries. The report is addressed to the Commission, the European Parliament and the Council, as well as to the public at large. In order to catch up with last year's backlog, the Working Party decided that the present report should exceptionally cover two years' developments, namely 2002 and 2003.

The seventh report continues the tradition of the previous reports as far as its structure is concerned. It gives an overview of main developments in the European Union, both in the Member States and at Community level and presents the issues addressed by the Working Party. The report further provides information about the main developments in third countries.

In 2002, the Working Party met five times and adopted 13 documents that were transmitted to the Commission and to the Article 31 Committee and, where appropriate, to the presidents of the Council, the European Parliament and others.

In 2003, the Working Party met six times and adopted 14 documents that were transmitted to the Commission and to the Article 31 Committee and, where appropriate, to the presidents of the Council, the European Parliament and others.

The Secretariat of the Article 29 Working Party is provided by the

European Commission
Directorate-General for the Internal Market
Data Protection Unit

The documents adopted by the Article 29 Working Party are available on this unit's web pages on the Europa server of the European Commission at the following addresses:

http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2002/wpdocs02_en.htm
http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm

General information on data protection is available on this site under:

http://europa.eu.int/comm/internal_market/privacy/index_en.htm

1. DEVELOPMENTS IN THE EUROPEAN UNION ON PRIVACY AND DATA PROTECTION

1.1. Directive 95/46/EC

1.1.1. Implementation into national law

Austria

Directive 95/46/EC was implemented in Austria in 1999 by the *Datenschutzgesetz* 2000 (DSG 2000), Federal Law Gazette, Part I, No 165/1999. It was amended once in 2001 to account for the conversion to the euro currency.

Belgium

The implementation law entered into force on 1 September 2001 (Belgian law of 8 December 1992 on privacy protection in relation to the processing of personal data, as modified by the law of 11 December 1998, implementing Directive 95/46/EC — http://www.privacy.fgov.be/textes_normatifs.htm).

The royal decree implementing the law was adopted on 13 February 2001 (Official Gazette, 13 March 2001), and entered into force six months after its publication, i.e. also on 1 September 2001.

In 2003, the law of 8 December 1992 was amended by a law of 26 February 2003. The amendments have as a main purpose the changing of statute of the Privacy Commission, which is no longer attached to the Ministry of Justice but to the Parliament.

The new legislation also foresees the creation of sector committees within the Privacy Commission; these committees will handle requests related to processing or communication of information subject to specific legislation (i.e. in the framework of e-government, social security, the national databank for mutual exchange of data on companies, and access to the public register of national identification (ID) numbers).

Denmark

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

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

Finland

Directive 95/46/EC 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 was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999. The act was revised on 1 December 2000, when provisions on the Commission's decision-making, as well as how binding these decisions are, in matters concerning the transfer of personal data to countries outside the Union under the data protection directive were incorporated into it.

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

France

The transposition into French law of Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data was on Parliament's agenda on several occasions in 2002 and 2003; in 2004, this work is now entering its final phase. The draft law amending the law of 6 January 1978 was adopted by the National Assembly in a first reading on 30 January 2002 and amended by the Senate on 1 April 2003. It was then adopted by the National Assembly in a second reading on 29 April 2004 and has been transmitted to the Senate for a second reading (session of 15 July 2004).

In the course of this work, the French legislator opted to avail itself of all the opportunities offered by Directive 95/46/EC. First of all, the draft introduces a simplification; in some cases, it even waives the prior formalities required of all personal data controllers. In a similar effort at simplification, but also for educational purposes, controllers may envisage appointing 'data protection officers', hence removing the need to notify the Commission nationale de l'informatique et des libertés (CNIL) in the case of processing subject to prior notification. On the other hand, certain so-called sensitive processing, whether this be in the public or the private sector, will be subject to an authorisation from the CNIL in nine specific cases: genetic and biometric data, criminal files, 'black lists', social case files, etc.

In addition, as a result of the changeover from a logic of prior checking to *ex post* checking, the CNIL will have its power to conduct *in situ* checks confirmed and extended. Lastly, it will be able to impose financial penalties or decide, in emergencies, to interrupt processing.

Finally, the draft provides that international transfers of data be authorised in advance by the CNIL and that this should be governed by a contract, or be subject to 'internal rules'.

Germany

In the course of modernising German data protection law, the federal government is following a two-phase approach.

The first phase was in substance directed towards implementing Directive 95/46/EC. On 14 June 2000, the federal government (*Bundeskabinett*) agreed on a draft law amending the German data protection law (BDSG). The Chamber of State Representatives (*Bundesrat*) made comments on this draft law on 29 September 2000. On 13 October 2000, the draft law amending the German data protection law and other laws was submitted by the federal government to the *Bundestag* (BT-Drs. 14/4329). Discussions in the various committees of the Federal Parliament (*Bundestag*) started in 2000 and were concluded by the law modifying the Federal Data Protection Act and other acts (*Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze*) as of 22 March 2001, Federal Law Gazette, Vol. I, p. 904. The text of the Federal Data Protection Act in the version which had been in force since 28 August 2002 was promulgated anew on 14 January 2003 (*Bekanntmachung der Neufassung des Bundesdatenschutzgesetzes vom 14. Januar 2003*, Federal Law Gazette, Vol. I, p. 66).

Subsequent to this 'novelisation', the second phase, which has already been started, is aiming at a fundamental reform of data protection law. An important step in this direction has been made by handing over the expert report on the modernisation of data protection law (*Modernisierung des Datenschutzrechts*) on 12 November 2001 to the Federal Ministry of the Interior.

Greece

Directive 95/46/EC has been implemented into national law by Law 2472/97 on the protection of individuals with regard to the processing of personal data (Official Gazette No A50/10-4-1997). Limited amendment of this law has been adopted by Article 8 of Law 2819/2000 (Official Gazette No 84/15-3-2000), providing exemptions to the notification obligation for some categories of data controllers. An English version of the amended text is available at www.dpa.gr.

Ireland

In December 2001, the European Communities data protection regulations 2001 transposed (with effect from 1 April 2002) Articles 4, 17, 25 and 27 of Directive 95/46/EC into Irish law.

The publication in February 2002 of the Data Protection (Amendment) Bill 2002 represented a major step towards the implementation of the directive in Ireland. The bill was passed by the Irish Senate in May 2002 but a general election in May 2002 and its consequential effects delayed passage of the bill. However, the bill was enacted by April 2003 and became effective from 1 July 2003 as the Data Protection (Amendment) Act 2003.

Italy

Directive 95/46/EC has already been transposed into national law by means of Act No 675/1996 as well as by subsequent legislation supplementing it. Transposition was ultimately finalised by the new Personal Data Protection Code (Legislative Decree No 196 of 30 June 2003), which entered into force on 1 January 2004.

The new Personal Data Protection Code consolidates all the legal provisions so far regulating personal data protection in Italy, thus considerably simplifying and harmonising the legal framework. Furthermore, the code has turned all these different provisions — laid down in different contexts and through various instruments — into primary legislation, thereby affording a high level of protection to the rights and freedoms concerned. Simplification, harmonisation and effectiveness are the underlying principles of the code with regard to exercise of data subjects' rights and the fulfilment of the relevant obligations by data controllers.

The code consists of three parts. In Part I, the general principles and obligations are set out that apply to all processing operations — except as specified in connection with some specific processing operations by the provisions contained in Part II that amend and/or supplement those laid down in Part I. Part III addresses the available remedies and lists the punishments provided for in case of non-compliance.

Among the most important provisions, reference can be made to Section 1 — which explicitly proclaims that everyone has the right to the protection of personal data, recently reaffirmed also by Article 8 of the Charter of Fundamental Rights of the European Union. Furthermore, Section 3 stresses the importance of the data minimisation principle in reducing the amount of personal and identification data, with regard both to information systems and software.

Several amendments and additions to the previous legislation were made by the code exactly in order to improve implementation of Directive 95/46/EC.

In particular, regarding national applicable law, the code transposed the Community principle focused on the controller's 'place of establishment' as per Article 4 of the directive, this being the main criterion for applying domestic law; therefore, the code regulates the processing of

personal data carried out by any entity that is 'established' in the State's territory also if it concerns data held abroad.

Simplification of the notification system was also completed further to the initial steps taken via Legislative Decree No 467/2001. Basically, the code reduced the scope of the requirements to be met by both private entities and the public administration.

In line with the directive, the mechanism applying to transborder data flows was also simplified, in particular by exempting controllers from the obligation to specifically notify the Garante per la protezione dei dati personali of data transfers if the processing of such data is not to be notified. In this manner, data controllers are no longer required to await expiry of the term previously provided for by the law in order to perform the transfers.

Additional amendments made by the code further to Parliament's intention to improve implementation of the directive concern the provisions on processing of sensitive data as well as the possibility for the Garante to draw not only the government's, but Parliament's attention as well to the appropriateness of introducing legislation required to ensure protection of fundamental human rights — as per Article 28(3), second indent, of the directive.

Luxembourg

Directive 95/46/EC was transposed into Luxembourg law by the law of 2 August 2002 regarding the protection of persons with regard to the processing of personal data. The law entered into force on 1 December 2002.

It contains provisions regarding a simplified notification procedure applicable to the most common and harmless data processing systems as well as an exemption of the notification duty for those data controllers who appoint a personal data protection official.

Several types of processing operations which are likely to present specific risks require prior authorisation by the national data protection authority, especially those:

- regarding sensitive data, health and genetic data;
- operated through interconnection of data or data processing systems;
- for other purposes than those for which the data have been collected;
- regarding credit and solvency of persons;
- for surveillance, for example, by means of video cameras;
- for surveillance by the employer of the workplace.

The national data protection authority, the Commission nationale pour la protection des données (CNPD), was set up in November 2002. A specific authority chaired by the chief public prosecutor is in charge of monitoring the application of the data protection provisions in the area of processing operations concerning public security, defence, State security, and prevention, detection and prosecution of criminal offences.

Netherlands

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

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

the supervisory authority changed from Registratiekamer into College bescherming persoonsgegevens (CBP). There is a great degree of continuity from one to the other act.

All new processing after that date had to comply with the new national data protection law, the *Wet bescherming persoonsgegevens* (WBP). There was a one-year transition period for existing processing, ending on 1 September 2002.

Portugal

The data protection directive was transposed into national law in 1998 by the Data Protection Act (Act 67/98) of 28 October 1998.

Spain

Directive 95/46/EC was incorporated into Spanish legislation under Organic Law 15/1999 on the protection of personal data (LOPD) (https://www.agpd.es/index.php?idSeccion=77). An English version can be found at https://www.agpd.es/index.php?idSeccion=347.

Sweden

Directive 95/46/EC was implemented in Sweden by the entry into force of the Personal Data Act (1998:204) on 24 October 1998 (http://www.datainspektionen.se/in_english).

Secondary legislation, i.e. the Personal Data Ordinance (1998:1191), came into force on the same day. The rules of Sections 9, 10, 13 and 21 of the new act shall not be applied before 1 October 2007 as regards manual processing of personal data that was commenced before 24 October 1998.

United Kingdom

The United Kingdom has implemented Directive 95/46/EC. The relevant national legislation is the Data Protection Act 1998 and associated regulations which came into force on 1 March 2000 (http://www.hmso.gov.uk/acts/acts1998/19980029.htm). The act establishes the role of the Information Commissioner as the independent data protection supervisory authority for the United Kingdom.

1.1.2. Infringement proceedings

In the data protection area, Luxembourg notified measures transposing Directive 95/46/EC (protection of individuals with regard to the processing of personal data and on the free movement of such data) on 21 August 2002, following a judgment given against it by the Court of Justice on 4 October 2001 ([2]).

In 2003, no Member State was taken to court.

([2]) Case C-450/00 *Commission* v *Luxembourg* [2001] ECR I-7069.

1.2. Directive 2002/58/EC

1.2.1. Implementation into national law

Austria

Directive 2002/58/EC has been adopted in the form of the new *Telekommunikationsgesetz* 2003 (TKG 2003 — Telecommunications Act 2003), Federal Law Gazette, Part I, No 70/2003. The fact that the TKG 2003 is meant to implement Directive 2002/58/EC is explicitly stated in Section 1, paragraph 4, subparagraph 5, of the TKG 2003.

Belgium

In 2002, no implementation took place. Directive 97/66/EC was transposed into national law as explained in the fourth annual report.

In 2003, the Belgian legislator transposed Article 13 of Directive 2002/58/EC into a law of 11 March 2003. The law provides for an 'opt-in' system for unsolicited electronic communications. Since 28 March 2003, the use of e-mails for marketing purposes has been forbidden without the prior, free, specific and informed consent of the recipients.

There are exceptions to this principle when the e-mail:

- has been directly communicated by a client to a company and is used only to inform this client of similar products or services of this company;
- is sent to a legal entity on condition that the e-mail address used is not personal (i.e. 'info@privacy.fgov.be' but not 'james.smith@privacy.fgov.be').

Denmark

The directive was transposed into national law in Denmark by:

- the Danish Constitution;
- the law on marketing practices, Section 6a (see Law No 450 of 10 June 2003);
- Law No 429 of 31 May 2000 on processing of personal data;
- the law on competitive conditions and consumer interests in the telecommunications market (see Executive Order No 661 of 10 July 2003), Section 34;
- Executive Order No 666 of 10 July 2003 on the provision of electronic communications networks and services;
- Chapter 71 of the law on administration of justice (see Executive Order No 777 of 16 September 2002);
- Section 263 of the Penal Code (see Executive Order No 779 of 16 September 2002).

Finland

The government bill on data protection of electronic communications was presented to Parliament on 24 October 2003. The law will implement Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector which was adopted in summer 2002. The aim is to bring the law into force as soon as possible after passing it.

France

The draft law on confidence in the digital economy (*loi pour la confiance dans l'économie numérique* — LCEN) which, *inter alia*, transposes the provisions on unsolicited electronic communications contained in the European directive on privacy and electronic communications of 12 July 2002 was adopted in a first reading by the National Assembly on 26 February 2003 and by the Senate on 25 June 2003. The law was finally adopted on 21 June 2004 after a decision of the Constitutional Council (10 June 2004) intervening after a second reading in the National Assembly (8 January 2004) and the Senate (8 April 2004).

The French Government asked the CNIL for its opinion on the preliminary draft law on 18 November 2002 and the latter submitted its opinion on this text on 28 November 2002. In addition, the CNIL was invited to outline its position on this text at regular hearings organised by each of the assemblies.

Germany

The directive has not been implemented up to now. But in the field of telecommunications, the new Telecommunications Act will enter into force in summer 2004. In the field of teleservices and media services, it is not clear when the directive will be implemented.

Greece

The procedure for the implementation of Directive 2000/58/EC into national law is not yet completed. Draft legislation is under discussion in the Ministry of Justice.

Ireland

Directive 97/66/EC was transposed into Irish law with effect from May 2002. In November 2003, its replacement Directive 2002/58/EC was transposed into Irish law by the Minister for Communications, Marine and Natural Resources via the European Communities (electronic communications networks and services) (data protection and privacy) regulations 2003.

Italy

The new Code on Personal Data Protection also implemented Directive 2002/58/EC, which replaced Directive 97/66/EC on data protection in the telecommunications sector; the latter directive had been transposed into Italy's national law by means of Legislative Decree No 171/1998 as amended by Legislative Decree No 467/2001. Title X, Sections 121 to 133, of the code specifically address electronic communications by transposing the new EC directive.

Directive 2002/58/EC introduced the opt-in — i.e. prior consent — principle as regards including a data subject's data into directories of subscribers to electronic communications services (Article 12) as well as sending unsolicited commercial communications (Article 13). The latter principle had actually already been implemented in Italy's legal system following transposition of the previous directive on telecommunications and privacy as well as of the directive on consumer protection in distance selling contracts.

Another innovation brought about by the Data Protection Code consists in the prohibition against using an electronic communications network to access information stored in a subscriber's/user's terminal equipment with a view to archiving information and/or monitoring the transactions carried out by the subscriber/user (e.g. via the so-called

'cookies'). New regulations were also laid down concerning processing of location data in respect of subscribers and users. Finally, more detailed, larger-scope provisions applying to unsolicited communications — so-called 'spamming' — were set out.

In this connection, it should be pointed out that data retention for the purpose of detecting and suppressing criminal offences was the subject of a lively parliamentary debate, which resulted in amendment of the code via a decree-law subsequently converted, with amendments, into Act No 45 of 26 February 2004. This act replaced the text of Section 132 of the code by providing that only data concerning telephone traffic may be retained for 24 months; they may be retained for longer exclusively with a view to detecting and suppressing some very serious criminal offences.

Luxembourg

Directive 2002/58/EC has not yet been transposed into national law.

The draft for a new bill regarding the specific rules governing the processing of personal data and the protection of privacy in the electronic communications sector will be examined by Parliament in late 2004.

It foresees mandatory traffic data retention by the operator of electronic communications networks during a period of one year for purposes of detection and prosecution of criminal offences. The operator is not entitled to use the data longer than necessary for operational and billing purposes, i.e. a maximum of six months.

Several provisions of the law regarding electronic commerce will also be modified in order to fully implement the directive.

Netherlands

Directive 2002/58/EC has been transposed into Dutch law mainly by the changed *Telecommunicatiewet* (Telecommunications Act), entering into force on 19 May 2004 ([3]). Other legislation transposing parts of this directive include the *Wet op de Economische Delicten* (Act on Economic Offences) that implements Article 13(4) of Directive 2002/58/EC. Deliberate breach of this regulation is a criminal offence under the Act on Economic Offences.

Portugal

Directive 2002/58/EC has not yet been transposed into national law. However, its Article 13 was already implemented in the act that transposes the e-commerce directive — Decree-Law 7/2004 of 7 January 2004.

Spain

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

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

Under the heading 'Secrecy of communications and protection of personal data and rights and obligations of a public nature linked to electronic communications networks and services' (Articles 33 to 38), Chapter III of Title III of the law contains a list of the rights of electronic networks and services consumers and end-users, highlighting the following where personal data protection is concerned.

Secrecy of communications (Article 33): In accordance with Articles 18.3 and 55.2 of the Spanish Constitution, operators of public electronic communications networks or providers of electronic communications services to the public must guarantee the secrecy of such communications and implement the required technical measures to this effect.

Protection of data of a personal nature (Article 34): In accordance with current legislation, operators of public electronic communications networks or providers of electronic communications services to the public must guarantee the protection of data of a personal nature in the course of their activity. These operators must take adequate technical and management measures to maintain the security of their network's operation or service provision, with the objective of guaranteeing the protection levels of data of a personal nature as required by the development norms of this law in this sphere.

Interception of electronic communications by technical services (Article 35): This may only occur in accordance with criminal proceedings law, when, to conduct monitoring tasks for the efficient use of the public radio-electronic domain, technical equipment, infrastructures and installations for signal interception not directed towards the general public are required, and only under the specific conditions stipulated by the law itself.

Encoding of networks and electronic communications services (Article 36): Any type of information transmitted through communications networks can be protected through encoding procedures. Encoding is a security instrument for information. Its conditions of use, when implemented for protecting the confidentiality of information, may include the obligation to provide a State general administration body or public authority with the algorithms or other encoding procedure employed, as well as the obligation to provide the encoding devices at no cost for control purposes in accordance with current legislation.

Rights of consumers and end-users (Article 38.3): In particular, subscribers to electronic communications services will have the following rights: to be made anonymous or have their traffic data cancelled when they are no longer necessary for the purposes of sending a communication; to have their traffic data used for commercial ends or provision of value added services only when their informed consent has been given to such effect; to receive non-itemised invoices when so requested; to the handling of their localisation data as distinct from their traffic data only taking place after they have been made anonymous or have expressed their consent; to halt the automatic re-routeing of calls to their terminal by a third party; to prevent identification of their line in calls generated or identification of the line to another user making the call; to prevent identification of the line number in incoming calls and to reject unidentified incoming calls, and to not receive automatic calls, without human intervention or fax messages, for direct sales ends without having given their former informed consent to this effect.

In turn, the preparation and sale of directories of subscribers to electronic communications services and the provision of information services on them will be conducted under the regime of free competition, guaranteeing, in any event, that subscribers will have the right to protection of their personal data, including the right not to appear in the said directories.

Breach (Article 53): Section (z) of this article considers a serious or repeated breach of the rights awarded by Article 38.3 a very serious offence, except the one contained in Section (h),

breach of which will be governed by the sanctioning regime contained in Law 34/2002 of 11 July 2002 on information society services and electronic commerce.

An electronic version can be found at https://www.agpd.es/index.php?idSeccion=77. An unofficial English translation is posted at https://www.agpd.es/index.php?idSeccion=347.

Sweden

Directive 2002/58/EC was implemented into Swedish law by the Electronic Communications Act (2003:389), which entered into force on 25 July 2003. Article 13 of the directive regarding unsolicited communications will be implemented by amendments in the Marketing Practices Act (1995:450) and will enter into force on 1 April 2004.

United Kingdom

The United Kingdom has implemented Directive 2002/58/EC. The relevant national legislation is the privacy and electronic communications regulations which came into force on 11 December 2003 (http://www.hmso.gov.uk/si/si2003/20032426.htm).

1.2.2. Infringement proceedings

Directive 2002/58/EC was set to be transposed by a deadline of 31 October 2003.

Initially proceedings for non-transposition had been opened (in December 2003) against nine Member States: Belgium, Finland, France, Germany, Greece, Luxembourg, the Netherlands, Portugal and Sweden. For Sweden, it concerned only Article 13 of the directive. Sweden transposed this article at the beginning of March 2004 and the proceeding was closed subsequently (March/April 2004).

Currently (1 June 2004) infringement proceedings have been opened for non-transposition or incomplete transposition of Directive 2002/58/EC against eight of the (old) Member States: Belgium, Finland, France, Germany, Greece, Luxembourg, the Netherlands and Portugal. In France and the Netherlands, legislation has been adopted, but the Commission is still awaiting formal notification, after which the proceedings will be closed. In the Netherlands, the legislation entered into force on 19 May 2004; in France, it has not yet entered into force but it is expected this will be the case by the end of June. In Belgium and Portugal, only Article 13 of the directive has been transposed. In Germany, partial transposition has been made, but the legislation will enter into force only on 1 July 2004.

Therefore, for the moment, there are eight infringement proceedings (all for non-transposition or incomplete transposition) at the stage of reasoned opinions (letters sent on 1 April 2004, so the deadline for response is 1 June 2004). It is expected that the proceeding against the Netherlands could be closed in the current infringement round as the notification is expected any day.

For relevant press releases, IP/03/1633 and IP/04/0435, see also the web page http://europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/infringements/ip10404_435.pdf.

1.3. Issues addressed by the Article 29 Working Party

1.3.1. Transfer of data to third countries

1.3.1.1. UNITED STATES OF AMERICA

WORKING DOCUMENT ON FUNCTIONING OF THE SAFE HARBOUR AGREEMENT

In this working document, the Working Party provides some comments regarding the state of the implementation of the Commission's decision of 26 July 2000 concerning the Safe Harbour Agreement (SHA). After stating the need for cooperation of all the authorities concerned with a view to full implementation of the Safe Harbour Agreement, the working document states the need to enhance the knowledge of EU data subjects regarding the existence of possible infringements of Safe Harbour principles. In this document, the Working Party also requests to be provided with up-to-date information with particular regard to a few issues related to implementation of the Safe Harbour Agreement.

OPINION 6/2002 ON TRANSMISSION OF PASSENGER MANIFEST INFORMATION AND OTHER DATA FROM AIRLINES TO THE UNITED STATES

In the aftermath of the events of 11 September 2001, the United States adopted, on 19 November 2001, the Aviation and Transportation Security Act requiring airlines flying into their territory to transfer to them data relating to passengers and cabin crew (passenger manifest information), to be made electronically and completed before the plane takes off, at the latest 15 minutes after departure for passengers. On 14 May 2002, the United States adopted another law to enhance border security that requires airlines arriving and departing from the United States to transmit data relating to passengers and crew to the US Immigration and Naturalisation Service, with the same data and transmission requirement. In both cases, data could be shared by other US federal authorities.

The Working Party considers that the US requirements create problems with respect to Directive 95/46/EC, that transfers of data relating to persons not travelling to the United States should be ruled out in principle, and that other transmission of data from reservation and departure control systems relating to passengers and cabin crew could only be envisaged in accordance with the legislation of the Member States within the limits of Article 13 of the directive, while a common approach at EU level should be sought. The Working Party calls for caution as regards transfers of sensitive data, for the US authorities to ensure respect of the directive where they have direct access to data systems, and for a negotiated system satisfactorily laying out the conditions and guarantees for the processing of personal data, incorporating the 'third-pillar' dimension.

OPINION 4/2003 ON THE LEVEL OF PROTECTION ENSURED IN THE US FOR THE TRANSFER OF PASSENGERS' DATA*

Further to its previous opinion on this issue, the Working Party took note of the progress of the talks conducted by the Commission on this issue in order to establish the conditions that would allow the latter to adopt a decision recognising 'adequate protection' on the basis of Article 25(6) of Directive 95/46/EC, in particular of 'undertakings' of 22 May 2003 from the US Bureau of Customs and Border Protection and the US Transportation Security Administration. The Working Party assessed the level of protection ensured by the United States after the requested transmission by airlines of personal data concerning their passengers

and crew members on the basis of their law and international commitments, as described in the undertakings and as laid down in relevant law.

The Working Party drew attention to several data protection concerns arising from the transfer to US authorities of passenger PNR data. The main outstanding points concerned the purpose of the transfers, the principle of proportionality as regards the personal data to be transferred as well as the moment of transfers and the retention period, the processing of sensitive data, the importance of adopting a 'push' method of transfer, the strict control on further transfers to other government or foreign authorities, the guarantees for and rights of data subjects, the mechanism for enforcement and dispute settlement, and the level of commitments. The Working Party urged the Commission to take its views fully into account in its negotiations with the US authorities, while recognising that ultimately political judgments would be needed.

1.3.1.2. ARGENTINA

OPINION 4/2002 ON ADEQUATE LEVEL OF PROTECTION OF PERSONAL DATA IN ARGENTINA

Following the request from the Argentine Government for an adequacy finding, the Commission sought the opinion of the Working Party in this regard. The protection of personal data in Argentina results from a system combining different elements, like the constitutional recognition of the 'habeas data' right, the legal norms regulating this right, and the broad interpretation and application of these norms by the Argentine courts, in particular as regards the scope of these norms. In its opinion, the Working Party analyses the Argentine legal framework as regards the basic data protection principles and the enforcement mechanisms necessary to meet the standard of adequate countries. On the basis of its findings and the explanation and assurances given by the Argentine Government, the Working Party assumes that Argentina ensures an adequate level of protection.

1.3.1.3. GUERNSEY/ISLE OF MAN

OPINION 5/2003 ON THE LEVEL OF PROTECTION OF PERSONAL DATA IN GUERNSEY* AND OPINION 6/2003 ON THE LEVEL OF PROTECTION OF PERSONAL DATA IN THE ISLE OF MAN*

The Article 29 Working Party advised favourably on the level of protection afforded by Guernsey and the Isle of Man, UK territories which are not part of the European Union and therefore from the perspective of Directive 95/46/EC are considered 'third countries'.

As indicated by the opinions issued by the Article 29 Working Party, Guernsey and the Isle of Man have data protection laws which follow closely the provision of the UK Data Protection Act with independent data protection authorities to monitor compliance with the rules.

The European Commission therefore adopted in due process decisions which have the effect of joining these UK territories to the list of adequate third countries.

1.3.2. Binding corporate rules

WORKING DOCUMENT: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES: APPLYING ARTICLE 26(2) OF THE EU DATA PROTECTION DIRECTIVE TO BINDING CORPORATE RULES FOR INTERNATIONAL DATA TRANSFERS*

The adoption by the European Commission in 2001 of two decisions on standard contractual clauses for the transfer of personal data outside the European Economic Area (EEA) (both for the transfer of personal data to controllers and processors established abroad) increased data controllers' awareness of the need to adduce appropriate safeguards for the transfer of personal data to third countries. The adoption of these Commission decisions nevertheless also put additional pressure on the regulators to further facilitate the putting in place of these safeguards. This is the origin of the so-called 'alternative standard contractual clauses' on which the Article 29 Working Party issued an opinion at the end of 2003 (see below) and is also the origin of the debate on the so-called 'binding corporate rules', i.e. codes of conduct for the transfer of personal data to third countries.

The discussions of the Article 29 Working Party, both at the subgroup 'standard contractual clauses' and at the plenary levels, took place over one year and were finalised with the adoption of a working document which is being considered as a 'new route' for the transfer of personal data to third countries although it left some questions open and was supposed to be followed up (see, for example, the relationship with the standard contractual clauses or the cooperation procedure for EU approval).

Binding corporate rules are self-regulatory data protection safeguards which are expected to be put in place by multinational companies on the basis of their own needs and business culture. They share the same principles of protection as the standard contractual clauses but enjoy greater flexibility, in particular as regards the participation of numerous subsidiaries around the globe. Binding corporate rules are expected to be enforced internally and grant third-party beneficiary rights to individuals who may, if necessary, enforce them vis-à-vis the data protection authorities or courts.

1.3.3. Standard contractual clauses

OPINION 8/2003 ON THE DRAFT STANDARD CONTRACTUAL CLAUSES SUBMITTED BY A GROUP OF BUSINESS ASSOCIATIONS ('THE ALTERNATIVE MODEL CONTRACT')*

The International Chamber of Commerce was one of the business associations most critically involved with the standard contractual clauses for transfers to data controllers adopted by the European Commission in mid-2001. At that time, the Commission made it clear that the model being adopted would not prevent it from adopting other models submitted by business associations in the presence of appropriate safeguards. The International Chamber of Commerce took up the challenge and, in coalition with other important business associations (Federation of European Direct Marketing (FEDMA), Japan Business Council in Europe (JBCE), Confederation of British Industry (CBI), Amcham, etc.), submitted 'alternative' standard contractual clauses for the consideration of the Commission at the beginning of 2002.

During 2002 and 2003, the subgroup 'standard contractual clauses' worked closely with the authors of the clauses and the Commission on the different version of the alternative standard contractual clauses being proposed by the business associations. Progressively, the differences in views of the representatives of the data protection authorities and the representatives of the business associations were narrowed down and the progress of dialogue was finalised by the adoption of a positive opinion by the Article 29 Working Party in December 2003.

The Article 29 Working Party's opinion invites the European Commission to endorse the business proposal as long as three main reservations are overcome: better cooperation with data protection authorities; right of access for citizens closer to the Commission's model; and more clarification on the system of liability designed by the alternative model.

1.3.4. Internet and telecommunications

WORKING DOCUMENT ON DETERMINING THE INTERNATIONAL APPLICATION OF EU DATA PROTECTION LAW TO PERSONAL DATA PROCESSING ON THE INTERNET BY NON-EU-BASED WEBSITES

Article 4(1)(c) of the data protection directive sets forth a rule on applicable law according to which EU data protection law applies when the data controller is not established on Community territory but makes use of equipment situated in the EU. The WP 56 document intends to clarify the application of this rule to online processing of personal data by data controllers established outside the Community. In this regard, the WP 56 document gives some guidance on the interpretation of the basic concepts used in Article 4(1)(c), such as the expressions 'equipment', 'make use of equipment', etc. Finally, it gives some clear examples of online processing of personal data by controllers established outside the EU which would be bound by the EU data protection legislation. One of the most representative examples is the collection by a data controller established outside the EU of personal data of individuals established in the EU by means of a text file (cookie), which is placed on the hard disk of the user's personal computer.

OPINION 2/2002 ON THE USE OF UNIQUE IDENTIFIERS IN TELECOMMUNICATION TERMINAL EQUIPMENT: THE EXAMPLE OF IPV6

In this opinion, the Working Party expressed its concerns regarding the possibility of the integration of a unique identification number into IP addresses. The opinion goes on to say that the unique identifier of an interface, such as the one that might be integrated into IPv6, would constitute an identifier the collection of which would be governed by data protection legislation. The opinion also recalls that telecommunications infrastructure and technical devices applications and design of new telecommunication devices should be privacy compliant by default, i.e. they should be designed in a way that either no personal data at all or as few personal data as technically possible are used to run networks and services.

WORKING DOCUMENT — FIRST ORIENTATIONS OF THE ARTICLE 29 WORKING PARTY CONCERNING ONLINE AUTHENTICATION SERVICES AND WORKING DOCUMENT ON ONLINE AUTHENTICATION SERVICES*

These two papers deal with online authentication services and particularly with privacy issues related to the Microsoft passport service and with Liberty Alliance specifications for online authentication.

As far as the passport service is concerned, the paper describes some modifications to be made to this service, including radical changes in the information data flow, in order to comply with data protection requirements. The paper sets forth some deadlines for Microsoft to implement the various changes to its passport service and it states that the Working Party will monitor such implementation. Finally, the paper refers to the expressed commitment of Microsoft to substantially modify the .NET Passport system.

The document also contains a chapter on the Liberty Alliance project, which is an ad hoc project in which different companies participate with the aim of establishing open standards for federated network identity through open technical specifications. The document contains some first considerations as to the issues that could be at stake at this stage of development of the project and in the future and guidelines of general application for any present or future online authentication system. In the paper, the Working Party asked Liberty Alliance to be informed about future steps regarding the adoption of specifications in order to ensure that the requirements of the data protection directive are taken into account.

OPINION 5/2002 ON THE STATEMENT OF THE EUROPEAN DATA PROTECTION COMMISSIONERS AT THE INTERNATIONAL CONFERENCE IN CARDIFF (9–11 SEPTEMBER 2002) ON MANDATORY SYSTEMATIC RETENTION OF TELECOMMUNICATION TRAFFIC DATA

In this opinion, the European data protection commissioners express their doubts about the legitimacy and legality of broad rules that would impose the systematic retention of traffic data concerning all kinds of telecommunication (i.e. details about time, place and numbers used for phone, fax, e-mail and other use of the Internet) for long periods of time (such as one year or more) in order to permit possible access by law enforcement and security bodies. The commissioners recall that, for such measures to be in accordance with data protection legislation, they must comply with the strict conditions set out by Article 15(1) of Directive 2002/58/EC of 12 July 2002 on privacy in the electronic communications sector, i.e. in each case, only for a limited period and, where necessary, appropriate and proportionate in a democratic society, which is not likely to be complied with by a rule that mandates a systematic retention of data.

OPINION 1/2003 ON THE STORAGE OF TRAFFIC DATA FOR BILLING PURPOSES*

This opinion provides some guidance to interpret Article 6 of Directive 2002/58/EC, which provides that the processing of traffic necessary for the purposes of subscriber billing and interconnection is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued. In particular, the opinion states that the period of time during which the bill may be lawfully challenged should be understood to mean a maximum storage period of three to six months. The opinion adds that, in such cases where the bill has been paid, a longer storage period might possibly be justified in exceptional cases where there are concrete indications that a dispute or query is to arise. The opinion emphasises that the stored traffic data must be limited to the 'necessary data'. Finally, the opinion rejects the argument that taxation purposes may legitimise the storage for longer time of traffic data used for billing. In this regard, the opinion explains that, while it may be necessary to keep proof of the bill for taxation purposes, this requirement should not be extended to the underlying traffic data on which telephone bills are based.

OPINION 2/2003 ON THE APPLICATION OF THE DATA PROTECTION PRINCIPLES TO THE WHOIS DIRECTORIES*

On 13 June 2003, the Working Party adopted Opinion 2/2003 on the application of the data protection principles to the Whois directories. In this opinion, the Working Party gives some guidelines to the Internet Corporation for Assigned Names and Numbers (ICANN) about the application of data protection principles to the Whois directories as well as to other registries of domain names and IP addresses. Amongst others, the opinion establishes that the publication in Whois registers of the identity and contact information of individuals without their consent violates the data protection directive in so far as there are no legal grounds justifying the mandatory publication of personal data referring to the individual. The opinion explains that such a publication of the personal data of individuals, for instance their

addresses and their telephone numbers, would conflict with their right to determine whether their personal data are included in a public directory and if so which. The opinion also stresses that the processing of personal data in reverse directories or multi-criteria searching services without unambiguous and informed consent by the individual is unfair and unlawful.

1.3.5. Codes of conduct

OPINION 1/2002 ON THE CEN/ISSS REPORT ON PRIVACY STANDARDISATION IN EUROPE

Privacy standardisation in Europe (PSE) has as its main objective to analyse the current status of privacy protection efforts and determine whether standardisation actions in the broadest sense could benefit the processes and implementation of the data protection directive. In this opinion, the Working Party welcomes the final report reviewing the possible role of standardisation in realising privacy and data protection in accordance with that directive.

OPINION 3/2003 ON THE EUROPEAN CODE OF CONDUCT OF FEDMA FOR THE USE OF PERSONAL DATA IN DIRECT MARKETING*

This opinion states that the European code of conduct of FEDMA fulfils the requirements laid down in Article 27 of the data protection directive. It further states that the code of conduct is in accordance with that directive and provides sufficient added value to it by being sufficiently focused on the specific data protection questions and problems in the direct marketing sector and offering sufficiently clear solutions to the questions and problems at stake. The opinion finishes by inviting FEDMA to produce an annex to the code dealing with online marketing issues, which are not addressed in the code.

1.3.6. Employment

WORKING DOCUMENT ON THE SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE

In 2001, the Article 29 Working Party made a substantial contribution to the processing of personal data in the employment context with the adoption of Opinion 8/2001, a general opinion which reviewed most of the data protection issues at work and which was meant to assist the preparatory work of the European Commission with a view to Community action in this area.

The working document on the surveillance of electronic communications in the workplace can be considered as a follow-up to the previous opinion and focuses on the conditions and limitations for the monitoring of electronic communications (including electronic mail at home). The document strikes a balance between the legitimate expectations of privacy at work by the employees and the legitimate interests and business needs of the employer. It stresses the principles of transparency with the employees, and of proportionality, necessity and fairness with the staff.

The working document contains some practical recommendations such as providing workers with two e-mail accounts as well as a recommended minimum content for companies' Internet privacy policy.

1.3.7. Others

OPINION 3/2002 ON THE DATA PROTECTION PROVISIONS OF A COMMISSION PROPOSAL FOR A DIRECTIVE ON THE HARMONISATION OF THE LAWS, REGULATIONS AND ADMINISTRATIVE PROVISIONS OF THE MEMBER STATES CONCERNING CREDIT FOR CONSUMERS

This short opinion is the Article 29 Working Party's response to an early consultation exercised by the European Commission on a draft directive on consumer credit which was meant to have some data protection provisions.

The opinion of the group was that the Commission's proposals could be either simplified with a reference to the provisions of Directive 95/46/EC or they would need to be further elaborated.

WORKING DOCUMENT ON BLACK LISTS

In this working document, the Article 29 Working Party was confronted with an issue of enormous complexity: blacklisting. The group reviewed the situation in the Member States as regards processing operations which were very likely to create prejudice to individuals such as doctors' records and solvency and credit information systems, criminal records databases, and fraud detection, *inter alia*. The document contains some conclusions and recommendations which stress the high risks that these databases pose for the fundamental rights and freedoms of individuals and also the existence of substantial differences among the Member States and therefore the need for further harmonisation at EU level in the future.

WORKING DOCUMENT ON THE PROCESSING OF PERSONAL DATA BY MEANS OF VIDEO SURVEILLANCE

Processing of personal data by means of video surveillance is a category of processing operations which shows clear differences with other processing operations. The personal data being processed are not of a textual nature but a combination of sound and image. The working document reaffirms the application of all provisions of the data protection directive to these processing operations but at the same time provides some advice on how to apply and interpret these provisions in view of the peculiarities of the personal data being processed.

This working document also contains a compilation of all national provisions applying to the processing of personal data by means of video surveillance.

The document was subject to public consultation during 2002–03, which led to the integration of some of the comments received and the adoption of Opinion 4/2004 with an identical title.

WORKING DOCUMENT ON E-GOVERNMENT*

This working document describes the existing e-government activities in different Member States such as the provision of electronic identity cards, online income tax declaration, administrative declaration of change of address, etc. In particular, the working document looks into the application of some of the requirements of the data protection directive to the provision of such e-government activities which entail the processing of personal data. In this regard, the document points out to what extent the national data protection authorities have been consulted by their respective governments before the provision of the e-government service in order to ensure compliance with data protection requirements.

WORKING DOCUMENT ON BIOMETRICS*

On 1 August 2003, the Working Party adopted a working document on biometrics (WP 80). The purpose of the document is to contribute to the effective and homogeneous application of national provisions on data protection adopted in compliance with Directive 95/46/EC in relation to biometric systems. The document focuses primarily on biometric applications for authentication and verification purposes, but aims also to provide uniform European guidelines, particularly for the biometric system industry and users of such technology. It stresses the particular nature of biometrics, *inter alia* the ability to collect biometric data without the knowledge of the data subject. In this perspective, the Working Party notes its clear preference for biometric applications that do not process biometric data unknowingly left by individuals or that are not kept in a centralised system. This should allow the data subject to exercise better control of the biometric data processed about him or her.

The Working Party concludes that, while the responsibility to develop biometric systems that are data protection compliant remains with industry, a working dialogue between all interested parties, in particular on the basis of a draft code of conduct, would be of great benefit.

OPINION 7/2003 ON THE REUSE OF PUBLIC SECTOR INFORMATION AND THE PROTECTION OF PERSONAL DATA*

This opinion provides guidance regarding the application of the requirements of the data protection directive which will have to be complied with by public sector bodies that are requested to disclose personal data for reuse purposes. The opinion was provided following the adoption of a draft directive on the reuse of public sector documents setting forth minimum harmonisation of the rules on the reuse of public sector information in the EU. After a description of the possible legal grounds that would legitimise the disclosure of public documents, the opinion focuses on the application of the purpose limitation principle.

1.4. Main developments in Member State countries concerning

A. Legislative measures adopted under the first pillar (this is excluding Directives 95/46/EC and 2002/58/EC)

B. Changes made under the second and third pillars

C. Major case-law

D. Specific issues

E. Website

Austria

A. Legislative measures adopted under the first pillar

Section 151 of the Industrial Code 1994, the regulation for direct marketing, was amended in 2002 (Federal Law Gazette, Part I, No 111/2002). The new regulation introduces more detailed provisions in order to establish a balance between the interest of direct marketing companies to collect and use personal data for direct mailing and the data protection interests of the data subject. Apart from a 'Robinson list' for people who do not want to receive direct mail, the principle is established that data subjects can demand deletion from the marketing lists of everyone, i.e. also of non-direct marketing companies.

A problem, which might need further legislative measures, is the use of electronic addresses for direct marketing purposes.

B. Changes made under the second and third pillars

Any major attempts for legislation in this field, as, for example, on mandatory traffic data retention, could be unsuccessful.

C. Major case-law

The use of data contained in the Austrian Central Residents Register (*Zentrales Melderegister*) caused some discussion in 2002 and 2003. The Ministry of the Interior made data from the register available to organisations in the private sector (lawyers, notaries and banks) that needed these data to file claims in court. This practice was basically legal, but there were allegations of abuse. The Data Protection Commission (DPC) issued a recommendation under Section 30, paragraph 6, of the DSG 2000, which addressed several problem areas. The Ministry of the Interior improved the search function and withdrew the access rights of companies that had abused the system. The text of the recommendation is available online (http://www.bka.gv.at/datenschutz/p30_zmr.htm).

The case of the direct marketing CD-ROM (see 'Specific issues') led to a number of complaints, mostly about the right to information.

A citizen desiring a health-related tax exemption was examined by a government physician (*Amtsarzt*) who judged the medical problem to be severe enough that the citizen's ability to drive a car should be checked by the competent authorities. He therefore reported the citizen's condition to the authorities responsible for driving licences. The Data Protection Commission finally concluded that the transmission was legal, because it was in the vital interest of the data subject himself.

The Austrian police force has a filing system to keep track of its paper files. This filing system contains records of charges brought against persons, but does not contain information about what became of these charges. Several citizens who had been accused of wrongdoing but not sentenced by a court demanded that their data be deleted. The Data Protection Commission ruled that the entries had to be updated with information on the outcome of the case.

D. Specific issues

Direct marketing

Cases involving direct marketing were common in 2002 and 2003. The Data Protection Commission had to give information and advice to citizens on their rights many times.

The most notorious incident happened in summer 2003, when a widely known direct marketing company announced that it would offer a collection of personal data for marketing purposes on CD-ROM, which caused an uproar in the media, following some statements from the non-governmental organisation (NGO) side about the infringement of citizens' rights.

The Data Protection Commission examined the project and made the following conditions mandatory for registration of the CD-ROM.

(a) The legal obligations existing in Austrian law for direct marketing companies must be transferred by contract to any user/buyer of the CD-ROM, as such user/buyer practically obtains a role which was hitherto reserved to direct marketing companies. This is especially important concerning the right to deletion from marketing lists drawn up by the user/buyer of the CD-ROM.

(b) The selection criteria, technically possible on the CD-ROM, must not allow for direct search for identifiable persons; for example, for the (or those) person(s) living at an exact address.

(c) Marketing analysis data, which are not 'hard facts' but (statistical) assumptions, must not infringe the sphere of privacy of the data subject. The DPC therefore refused, for example, to register analysis data classifying the relationship between people living at the same address as 'partners' or otherwise as 'family members'.

E. Website

The website of the Austrian Data Protection Commission is still at www.bka.gv.at/datenschutz. A change to a new address (www.dsk.gv.at) is planned. Please keep an eye on the site.

Belgium

A. Legislative measures adopted under the first pillar

Law of 22 August 2002 on the rights of patients

The Privacy Commission has already given an opinion (No 30/2001) on this legislation, mentioned in the sixth annual report.

As regards privacy aspects, the text foresees, in particular, a right to be informed on one's state of health, conditions of access to the medical file, and conditions of access by members of the family to the medical file of a deceased person. The comments of the Commission focused mainly on the need for a better balance between the discretionary power of the doctor and the right of the patient (or his/her parents) as regards the right to get information about the content of the medical file.

Another aspect of the legislation relates to the medical data that can be communicated to insurance companies in the framework of the conclusion of a contract. The text restricts the quality of medical data that could be transmitted to insurance companies.

Law of 25 March 2003 on the national register
This law provides for new conditions of access to the information in the national register, and regarding the use of the national ID number.

As stated in Section 1.1, the Privacy Commission has a specific competence to authorise access and use of the information, on a case-by-case basis and through the issuance of official authorisations.

B. Changes made under the second and third pillars

A law on cybercrime was adopted on 28 November 2000, and published in the Official Gazette of 3 February 2001. The law foresees that traffic data shall be stored a priori by telecommunications operators and service providers for a minimum of one year. This provision has been decided against the official opinion of the Commission.

This provision is still not in force as no secondary legislation has yet been adopted to determine the exact duration of storage.

In 2003, the federal police were working on a new information handling policy which has not yet been finalised. A new internal control and audit organ was set up inside the federal police. This organ acts as an internal data protection officer for police law enforcement authorities. It is not considered as an independent authority because it is not under the authority of the Parliament, but it can provide useful assistance to the Commission in this specific sector. Another organ of control put in place in 2003, similar to this data protection supervisor, is the general inspection service of the police forces. Like the supervisor, it depends directly on the Ministry of Internal Affairs (this organ comes in addition to the permanent Committee of the Police Services which since 1993 has been under the authority of the Parliament).

C. Major case-law

No major developments to be mentioned.

D. Specific issues

Recording of telephone communications by banks
The conditions of recording of communications between clients and their banks were subject to large debate in the media in the course of 2002.

At the origin of this debate was the initiative of a bank to send to all its clients information stating that their communications with the services of the bank would be recorded.

The Commission considered it useful to get a global picture of the recording practices in this sector, and sent to all major banks in Belgium a list of questions on their practices.

In all, 50 of 55 banks described their practices to the Commission. On the basis of this information, the Commission published an opinion on 22 August 2002 analysing the

recording practices in the banking sector and emphasising the need for better compliance with regard to some aspects of the data processing.

In particular, the Commission considered that most of the recording takes place in specific circumstances and is justified, mostly with respect to the necessity for the bank to keep a proof of transactions (especially with regard to phone banking and stock exchange operations).

It was raised, however, that the processing often lacks transparency.

The Commission considered it necessary to recall that, to be lawful, recording must comply with the following obligations:

- clear and complete information on the conditions of recording;
- obtention of the free and explicit consent of the persons concerned, on the basis of this information;
- storage of recordings for a period not longer than the period during which the transaction can be contested (three months being considered as a reasonable period);
- physical and organisational security measures in order to avoid unlawful reuse of the data.

Children and the Internet

The Commission adopted on 16 September 2002 an official opinion on the protection of children on the Internet.

The objective of this opinion is to clarify the way data protection legislation applies to minors on the Internet, considering the specific weakness of their position.

It was drafted during close contacts with the Internet Rights Observatory, newly established within the Ministry of Economic Affairs. It is intended to give wide publicity both to the conclusions of the Commission and the Observatory.

The first part of the opinion provides for a strict interpretation of the principles of the law in order to protect the rights of children.

- As regards the transparency principle, the opinion focuses on the need for simple and accessible information on the rights of the child, and suggests that the child be encouraged to discuss Internet issues with his/her parents.

- As regards the necessity principle, it is recommended that no identifiable information is collected on children (photos, physical address, name of school, etc.). The Commission insists on the limits to the reuse or transfer to third parties of personal data of children.

- As regards the fairness principle, it is considered illegal to collect from a child information about his/her family or friends and to collect information in the course of a game or in exchange for a present. Marketing should not be directed to children under the age of judgment. The opinion recalls the specific protection of sensitive data.

- A specific chapter focuses on the publication of school pictures and insists on the need for parental consent.

In a second part, the opinion addresses the question of online identification of visitors of websites not intended for children.

While the Data Protection Authority always insists on the need to preserve a possibility to surf anonymously on the Internet, it acknowledges that identification would be needed in order to prevent minors from accessing harmful material on the web.

In that perspective, the Commission insists on the need to encourage use of the less intrusive possible identification tools.

In particular, instead of transmitting copies of identity cards or credit card numbers, the opinion refers to the existing possibility to use pseudonym certificates in order, for example, to buy online. It is suggested to use this possibility to certify online that someone is under or

over 18 years of age in order to give that person access to some specific material, without disclosing directly his/her identity. The opinion ends by mentioning the necessity to combine privacy tools with other tools destined for the protection of children on the Internet, such as filtering software, labelling of sites, and information campaigns directed towards adults as well as children.

Spam box

The Belgian Privacy Commission has initiated a project on spam, including the creation of a spam box, in order to evaluate the phenomenon. A report was published in July 2003 together with a press release (http://www.privacy.fgov.be/sommaire.htm (press), http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf (analysis and practical guide)).

The report includes both the results of the 'spam box' action started in October 2002 and a guide explaining the new legislation.

As to the spam box, in two months, the Commission had received more than 50 000 e-mails. The Commission has analysed and classified them according to their origin and their subject.

Like the CNIL in France, the Belgian Privacy Commission noticed that a large majority of the e-mails came from the United States (86 % of the e-mails were in English) while only 2.8 % were identified as coming from Belgian senders and 3.2 % from the rest of Europe.

Based on this analysis, the Commission has taken the following measures:

- contact with 70 Belgian companies in order to draw their attention to the legislation applicable in this field and the warning of companies regarding the most serious infringements against legal proceedings; in addition, e-mails with paedophile content have been transferred to the Computer Crime Unit of the federal police;
- contact with Internet access providers in order to verify their policy regarding the management of the database of their clients' e-mail addresses; their attention was drawn to the legislation that protects the users and the utilisation of their e-mail addresses;
- transfer to other European data protection authorities of e-mails which seem to come from their country so that they can examine a possible infringement of their own legislation;
- identification of specific illegal e-mails coming from the United States, which were communicated to the US Federal Trade Commission;
- publication online of a practical guide for the senders and recipients of e-mails.

E-government

The process towards electronic circulation of information within the administration and between the administration and the public has already been mentioned in the fourth annual report.

In order to facilitate and accelerate the handling of information of individuals — as well as of companies — it has been decided to generalise the use of a unique identification number, attributed to each entity. This number will also be the reference integrated into the future electronic identity card.

The individual will be requested to use his/her card in all his/her contacts with the administration. He/she will also have the possibility to use it in order to electronically sign documents online (e.g. while completing online a VAT declaration).

While the general objectives and the efficiency aspects of the project cannot be questioned, issues have been raised by the Commission regarding the guarantees taken in order to limit the risks of abuse of the system, considering especially that one of its main goals is to facilitate the circulation of personal information between different administrative services. An official opinion was adopted in 2002 (19/2002), which mostly insisted on the need for protection of data included electronically in the new ID card, on the restrictive conditions of

access to personal data of the national register, and on use of the national identification number. Since 2004, the Commission has had specific competence in authorising on a case-by-case basis access to the database and utilisation of the national ID number (further to the law of 25 March 2003 on the national register).

E. Website

http://www.privacy.fgov.be

Denmark

A. Legislative measures adopted under the first pillar

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

The question whether a legislative measure that implies a reduction of the right to privacy, should be put forward is a matter to be decided by the Danish Parliament. In this connection, the DPA has noted that several bills in recent years have been passed, even though the DPA has pointed out that this would result in a reduction of the right to privacy.

In 2002, the DPA was asked to comment on the amendment of the Act on National Health Insurance. The purpose of the bill was to make an electronic register on individuals' purchase of pharmaceutical products and information related thereto — in short, a personal electronic pharmaceutical profile.

The DPA found that, in connection with the personal electronic pharmaceutical profile, a great amount of data would be collected, some of which would only be of use rarely if ever. On this basis, the DPA expressed doubt whether the necessary proportionality was present between the collection of data regarding all purchases of prescripted pharmaceutical products and the fulfilment of the purpose of the bill.

Seen in the light of the right to privacy, the DPA was of the opinion that the personal electronic pharmaceutical profile should only be established if great public interest were present.

Another case in 2002 concerned an amendment to the Act on Archives. The DPA was of the opinion that personal data, which have been obtained through access to an archive, should be dealt with in accordance with the Act on Processing of Personal Data, regardless of whether this obtainment takes place prior or later to the time limit of accessibility.

In 2003, the DPA evaluated a new legislative proposal concerning the establishment of a national register containing a record of at least one bank account number for every adult living in Denmark who receives payments from the Danish Government. As practically all citizens regularly receive payments in the form of tax returns or State welfare, the size of the register would be very large. The purpose of the register would be to ensure substantial governmental savings in the administration of such payments. The DPA noted two important

circumstances in connection with the establishment of the register, i.e. that registration was optional, and that the register was established in a way that the individual case worker in the public authority would not get access to the bank account numbers.

The DPA was also asked to make remarks on a report and a bill regarding openness in civil and penal proceedings. In this connection, the DPA stated that the concern of public administration of justice had to be carefully balanced against the concern of protecting sensitive personal data. In the DPA's view, the proposal had consequences relating to data protection and would amount to a reduction in the level of data protection.

B. Changes made under the second and third pillars

In 2002, the Danish Ministry of Justice requested the DPA to make remarks on a protocol to an amendment of the Europol Convention (Europol 76).

In conclusion, it was the view of the DPA that the amendment, if it were to be put forward, would result in significant changes of the Europol Convention. As a result of this, the DPA requested that the need for the proposed amendment should be carefully balanced against the consequences for the data protection that the amendment would bring.

In 2003, the Ministry of Justice proposed a bill concerning changes involving, for instance, the Penal Code, the Administration of Justice Act and the Marketing Practices Act.

One of the important changes concerned the protection against infringements of information in relation to software solutions. The DPA stated that, in the light of the citizens' increased use of software solutions, it regarded as an important element in the protection of the right to privacy that the Penal Code provide a sufficient safeguard against infringements of software solutions.

The other important change relates to the implementation of the Cybercrime Convention, and includes a change in the Administration of Justice Act, in order to make it possible for the police to order the telecommunication companies to store and save electronic data. The purpose of the amendment was to prevent electronic data of importance to an investigation from being deleted according to usual practice at the telecommunication companies. The DPA specified the concerns on data protection relating to the bill, and pointed out that a statutory basis should be provided, in order to make it possible for the telecommunication companies to save the electronic data. Among other things, the DPA put emphasis on the need to clarify who was to be considered the controller of the emergency secured data. In the proposed act, it is now stated that the police will be the controller, that Executive Order No 528 of 15 June 2000 concerning security in the processing of data of a public authority will apply, and the DPA will be competent to make inspections.

C. Major case-law

All cases concerning the Act on Processing of Personal Data were in 2002 decided administratively by the DPA. In one case, the DPA made a report to the police regarding violation of the Act on Processing of Personal Data.

The case dealt with a breach of the duty to provide the DPA with sufficient information, in order for the DPA to establish if there were a duty to make a notification to the DPA prior to

commencement of any processing of data which is carried out on behalf of a private controller. The controller accepted an out-of-court fine of DKK 500 which is approximately EUR 69.

In 2003, the DPA made a report to the police regarding violation of the Act on Processing of Personal Data in two cases.

The first case concerned an illegal transfer of data without explicit consent in connection with marketing. The controller accepted an out-of-court fine of DKK 7 000, which is approximately EUR 960, for both violations of the Act on Processing of Personal Data and the Marketing Practices Act.

The other case concerned an illegal gathering of data from a credit information agency and transfer of these data. The controller accepted an out-of-court fine of DKK 5 000, which is approximately EUR 685.

D. Specific issues

1. In 2002, the DPA declared that a trade union's planned publishing of a list of members on electronic media could only take place if the trade union had collected every member's explicit consent prior to the publishing. The same would apply if the publishing alternatively takes place on non-electronic media.

2. The DPA has also dealt with issues concerning a common register on claims in the insurance business. Here, the DPA concluded that the establishment of a national register on claims can take place only with the explicit consent of the policyholder.

3. The DPA also expressed its opinion on the publishing of pictures on the Internet of people in regular situations — hereby meaning, for example, children playing in the schoolyard. The DPA found that harmless pictures in certain circumstances can be published on the Internet without explicit consent. The publishing of pictures of employees and customers can, in most circumstances, take place only with explicit consent.

4. In connection with a blacklist of companies in the wood business, the DPA found that an environmental organisation's processing of data on a website was not carried out for the purpose of warning third parties against entering into business relations or an employment relationship with a data subject. Here, the DPA especially considered the right to freedom of expression.

5. With regard to live video transmissions in a pub, the DPA stated that the publishing of live recordings from a pub on the Internet with the purpose of marketing the pub can only take place if the persons involved have given their explicit consent. It was furthermore recommended that the video transmission was simultaneously shown on a screen in the pub.

6. The DPA also expressed its view on the processing of personal data in connection with an application for rent support. In this connection, explicit consent is a condition for the transfer of information about a person's income to other persons in the household.

It was the opinion of the DPA that merely the concern of a fast accomplishment of a digital solution should not amount to a deviation from the protection that a person has under the Act on Processing of Personal Data. Ideally, the solution should be that there be established a

self-service arrangement where the household member participates in the raising of electronic data if possible with the option of giving digital consent.

7. The DPA has handled a number of cases dealing with the security of processing. Several of these cases have been initiated on the DPA's own initiative.

In one case, the DPA has found that the so-called OCES certificates — a software solution — in general can be used when citizens send information to and receive information from public authorities, even if the information contains sensitive personal data. OCES certificates are defined by Danish authorities according to international standards, and are to be used as digital signatures and for encryption purposes.

8. In 2003, the DPA expressed the opinion that telecommunication companies are not allowed to transfer data about their customers to the Antipiratgruppen — an organisation fighting infringement of copyrights — without a court order. In all, the DPA found that, because of the fundamental and contradictory interests in the assessment, the question of handing over information about the customers was a question to be decided by judicial review.

9. The DPA also dealt with the issue of transfer of information from the passenger name record reservation system (PNR) to the US authorities. The DPA has granted an airline company permission to process information in Denmark and to transfer information to the United States on detailed conditions, stating amongst other things that the airline company only collects and transfers information indicating circumstances of a sensitive nature about the passengers to the US authorities, if explicit consent is obtained prior to the transfer, and the passenger is clearly informed about the transfer and other details mentioned in the granted permit.

10. With regard to publishing personal data on the Internet, the DPA stated that freedom of expression had to be taken into consideration. There has to be a balance of interests consisting of, on the one hand, the right to privacy and, on the other hand, the right to freedom of information and speech. In this connection, it has to be ensured that the Act on the Processing of Personal Data does not place restrictions on these fundamental freedoms.

11. The DPA also dealt with the issue of biometrics in the form of ferry passengers' fingerprints. In its decision, the DPA concluded that a fingerprint or the information about a calculated value of the measuring point of the passengers' fingerprints contained in the system was to be considered personal data covered by the Act on Processing of Personal Data. In addition, the DPA concluded that processing in the definition of the act took place, and that this under certain circumstances can be considered to be in compliance with the Act on Processing of Personal Data. In addition, the DPA put emphasis on the fact that the solution in question did not contain a central database with fingerprints.

12. In a case concerning video surveillance of employees, the DPA was of the opinion that the gathering of information by means of video surveillance carried out in order to create security and to prevent and investigate crime has a specified explicit and legitimate purpose.

However, according to the Act on Processing of Personal Data, it is a demand that data shall be processed in accordance with good practices for the processing of data. According to the explanatory notes to the statutory provision, the demand of good practices for the processing of data implies that the processing has to be reasonable and legal. Furthermore, it is stated that

a reasonable processing of data implies that it is possible for the data subject to obtain knowledge about the existence of the processing, and when data are gathered that the data subject gets accurate and adequate information about the circumstances in connection with the gathering of data.

In connection with video surveillance with the purpose of control, the DPA pointed out that it is a chief rule of the principle of good practices for the processing of data that the employee is given notification of the surveillance prior to the commencement thereof.

When assessing if the chief rule can be derogated from, the circumstances which are applied when considering a possible derogation from the rules of information to be provided to the data subject have to be taken into consideration. This could be vital to private or public interests.

13. The DPA has handled a number of cases dealing with the security of processing. Several of these have been initiated on the DPA's own initiative.

One of the cases in 2003 regarding security dealt with a breach in a wireless local area network (WLAN). In this connection, the DPA pointed out that any device in a wireless local area network is a potential target for attack. As a result, the DPA found that the controller already from the establishment of the network should have established a procedure to verify changes of configuration in the local area network.

E. Website

The website of the Danish Data Protection Agency is at www.datatilsynet.dk. It can be consulted in Danish and in English.

Finland

A. Legislative measures adopted under the first pillar

From the perspective of data protection, the significant acts enacted in 2002 include the Act on Offering Information Society Services (458/2002), the Private Security Services Act (282/2002), the Act on Checking the Criminal Background of Persons Working with Children (504/2002), the Act on Processing of Personal Data in the Execution of a Punishment (422/2002) and the Act on Background Checks (177/2002). The last emphasises the primary importance of general security work and stresses that the three levels of background checks carried out by the police in the personal data file are only a supplementary means in certain situations that are highly significant from the security point of view.

The year 2003 saw the enactment of, for instance, the Act on Electronic Services and Communication in the Public Sector (13/2003), the Act on the Amendment of the Identity Card Act (300/2003) and the Act on Electronic Signatures (14/2003). The last implemented the regulations of the European directive on electronic signatures. The year 2003 also saw the reform of acts on important registers controlled by the authorities, such as the Act on Processing of Personal Data in Police Action (761/2003) and the Act on the Vehicle Traffic Register (541/2003). The reason for amending these acts, as well as acts on social insurance, was partly to harmonise them with regulations on the processing of personal data. The reform of the Execution Act (680/2003) created a centrally governed national debt recovery procedure information system. In addition to increasing the right of authorities to receive information, both the reform of the Execution Act and the acts on the above registers also

increased the right to transfer information via a technological interface. In addition to the increase in the right to receive information without consent, the information structure, data transfer and security solutions of the data systems will become increasingly important. At the same time, the right of the data subjects to also be informed of the transfers in advance during the collection of personal data is emphasised.

In 2002 and 2003, the Data Protection Ombudsman was heard in approximately 50 legislative matters.

B. Changes made under the second and third pillars

Parliament passed the Act on Processing of Personal Data in Police Action (761/2003) on 22 August 2003. In Finland, the principles of the data protection directive are also applied in the processing of matters coming under the second and third pillars.

C. Major case-law

Data protection crimes and violations associated with the automatic processing of personal data were increasingly brought to the attention of the Data Protection Ombudsman in 2002 and 2003 in the form of various requests for a statement. Cases have also been taken to court for a decision by the parties concerned. There were alarmingly many cases of the use of large information and data transfer systems contrary to their intended use. Such cases were also discovered in checks carried out by two major governmental controllers with the help of log files. The cases, which received much publicity, increased public awareness of data protection and its risks and stressed the importance of protecting the registers.

During the evaluation related to the public transport information system of a couple of large cities, the Data Protection Ombudsman contemplated the necessity of defining the different personal data registers (different purposes of processing) included in the information system. Also the question as to whether the identity information associated with each individual travel card can be used to record every journey in the reading devices connected with the central system was assessed. Following a request by the Data Protection Ombudsman, the controller removed the possibility of collecting and recording journey data on an identifiable individual passenger, as it was contrary to the necessity requirement of the Personal Data Act. Furthermore, it was evaluated whether the personal identity code of those who had bought a travel card was necessary in the customer register when the individual had not chosen the anonymous but also more expensive card. The Data Protection Board, which dealt with the issue of personal identity codes, deemed the collection and recording of personal identity codes necessary, because the controller needed them in order to ascertain the home municipality of the travel card users, as the different municipalities of the district participate in the maintenance of public transport according to different criteria. Furthermore, the travel card service also includes the possibility of entering a card on a 'hot' card list and being reimbursed for the value of a lost or stolen travel card.

The Data Protection Ombudsman applied to the Data Protection Board to prohibit the processing of personal data by a company that collected taxation information on individuals and published them regionally as a 'magazine' and by another company, owned by the same group, which offered taxation information based on information on the said publication as an SMS service. The Data Protection Board returned an unfavourable decision, mainly on the basis of freedom of speech. The Data Protection Ombudsman has appealed the decision to the Administrative Court. The appeal included a request that the competent Administrative Court request a preliminary ruling from the Court of Justice of the European Communities.

E-mail confidentiality was at issue in a dispute between some teleoperators, in which telecommunication identification data associated with service agreements between operators

were suspected of being used for direct marketing, contrary to law. In a similar vein, abuse of telecommunication identification data by a large teleoperator was uncovered. Certain people employed by the teleoperator were suspected of using telecommunication identification data for their own monitoring purposes in contravention of the Personal Data Act.

D. Specific issues

In Finland, as elsewhere, data protection has sought its own place in the versatile field of rights and phenomena. The issue, often understood as vertical and rather detached, is clearly becoming a more horizontal branch of jurisdiction, associated with surrounding phenomena and networks.

The Office of the Data Protection Ombudsman has stressed considering the significance of the Personal Data Act and protection of privacy as a builder of confidence among data subjects and as a success factor for business enterprises. Indeed, the importance of providing information to data subjects in e-transactions and services will become increasingly prominent. Research shows the task to be challenging. In summer 2003, the Office of the Data Protection Ombudsman carried out a study, with the working title 'The Internet police', which surveyed 500 websites from the perspective of the duty of providing information referred to in Section 24 of the Personal Data Act. The survey showed that only approximately 10 % of administrative websites provided information on the processing of personal data collected over the Internet. Webzines fared best, with nearly 80 % incorporating at least some information required by Section 24 of the Personal Data Act. After the survey, the Office of the Data Protection Ombudsman distributed brochures to data subjects and data protection guides to municipalities, central administration, non-governmental and labour organisations and trade and employers' associations, among others. The Office of the Data Protection Ombudsman used this context to draw special attention to the duty of providing information referred to in the Personal Data Act.

The year 2003 made history by being the worst computer virus year to date. These viruses and malware, known by many different names, were characterised by the fact that they spread faster and wider than ever before and that they also created a threat to the infrastructure of society. For instance, a bank was forced to close its doors temporarily and the e-mail traffic of a teleoperator was completely jammed.

In addition to viruses, mobile phone and e-mail users were plagued by consistently high levels of junk mail, which, however, still mainly originated outside Finland, predominantly in the United States. The Market Court gave a decision in June, which further defined the concept of 'spam'. According to the Court, using e-mail to request the prior consent required by law is already to be considered marketing. It was hoped that a government bill on the data protection of electronic communications, prepared by the Ministry of Transport and Communications, would help in the battle against malware and junk mail. The above cases undoubtedly increased public awareness of data security, though, at the same time, confidence in the security of networks decreased.

Government authorities have given more prominence to data protection in development and coordination activities across different administrative branches. Society has also reacted strongly to viruses and other data security problems.

At the end of 2003, the Council of State adopted an information society programme. The programme's implementation plan incorporates legislative requirements pertaining to the processing of personal data (data protection) in all development activities. The programme includes the idea that the confidence of citizens and companies in the services offered by the information society will be promoted by improving data security and protection of privacy.

The Data Protection Ombudsman was invited to be a permanent expert member of the Information Society Council.

On 4 September 2003, the Council of State adopted a decision in principle on the national data security strategy. The strategy is based on a proposal by an advisory board on data security issues, which was active in 2001–03. One of the starting points in the proposal is safeguarding citizens' fundamental rights, such as protection of personal data. The Ministry of Transport and Communications was later awarded a prize by the RSA Data Security Conference for the best European security concept.

The Steering Committee for Data Security in State Administration (VAHTI), attached to the Ministry of Finance, was also active during this period. It prepared and published many guidelines that proved to be 'bestsellers'. The Data Protection Ombudsman and many experts from his Office also participated in preparing these guidelines.

The debate about the use of the personal identity code has been partly replaced with questions concerned with electronic identity codes and biometric identification systems. There was lively debate in connection with the amendment of the Identity Card Act on the 'one-card principle', meaning that data normally recorded on a health insurance card could be recorded on a personal identity card. According to the stance emphasising the right of self-determination, also advocated by the Data Protection Ombudsman, the legislative solution was that health insurance card data can be incorporated into a personal identity card, which also serves as a travel document, only by request of the cardholder and if the cardholder is duly informed about the significance of including such data on the personal identity card.

Data protection issues are being increasingly focused upon in education. There is also increasing awareness of the need to include data protection and data security issues in the curricula of various educational institutions. The Office of the Data Protection Ombudsman, education authorities and other central expert bodies and organisations began the production of educational material for comprehensive schools and upper secondary schools in particular.

The social and health administration began an extensive healthcare development project, part of which consists of developing a national electronic patient documentation system. The project aims at using a uniform data structure and compatible technology to create a system enabling the various healthcare units to transfer data nationally and regionally, subject to the consent of the patient.

E. Website

www.tietosuoja.fi

France

A. Legislative measures adopted under the first pillar

Implementation of right of direct access to medical files by patients

The law of 4 March 2002 relative to patients' rights and the quality of the health system has changed the rules of access of patients to their medical files. So far, the rule was that such access could be made only indirectly through a medical practitioner. This law has changed this principle: the patient may not exert this right directly, and the decree of 29 April 2002 has organised this access.

However, the patient may still, if he/she so wishes, have access to his/her medical data by requesting a doctor to do so on his/her behalf.

This communication must be effective within eight days following the access request and at the earliest after 48 hours have elapsed. If these data were collected more than five years ago, this time period is set at two months. This time period starts from the date on which the medical information was constituted. The presence of a third party may be recommended by the doctor but he/she may not forbid direct access to the file in case the patient refuses to follow this recommendation.

B. Legislative measures adopted under the second and third pillars

Law on internal security

On 23 September 2002, the Minister for the Interior, Internal Security and Local Freedoms presented the draft law on internal security in the Council of Ministers. Although some of the provisions of this text fall directly within the scope of the data protection law of 6 January 1978, the CNIL had not been consulted on the preliminary draft law. However, at its meeting of 24 October 2002, it concluded that it should make its position known to the government and to Parliament. This is the first time in the history of the CNIL that it has acted of its own motion in respect of a draft law.

The main impact of this new legislation on the protection of personal data falls into four categories.

Firstly, it provides a legal basis for the existence of the files of the Criminal Investigation Department, defines their boundaries and characteristics and the recipients in France, while also defining the non-national or international bodies which may be recipients of personal data processed and recorded in these files.

Secondly, and more critical in the CNIL's view, the new law further expands the cases in which judicial police files can be consulted for purely administrative purposes. On this question, the CNIL pointed out that such an expansion risked having these files play the role of parallel criminal records, without offering in return either the guarantees or the control procedures which currently apply to the updating and administration of the automated file of criminal records.

Thirdly, the law widens the list of offences giving rise to inclusion in the national genetic fingerprint file (FNAEG). It also provides for the possibility of retaining the genetic fingerprints of persons where there are one or more plausible reasons to suspect that they have committed one of these offences and for recording in this file the genetic stains collected during procedures to investigate the cause of a death or of a disappearance and any genetic fingerprints which correspond or may correspond to those of deceased or missing persons.

Lastly, the law removes the right of persons suspected of having committed such an offence to refuse to submit to having a sample taken.

The CNIL will need to deliver an opinion on some of the texts implementing this law.

Law on immigration

Under a tighter immigration policy, the immigration law of 24 November 2003 has substantially reformed the procedures for checking identities when issuing visas and carrying out checks at borders, with wide recourse to biometric techniques.

The new law extends the possibility, available since 1997, of recording and processing the fingerprints of non-nationals who, in the course of checks at border crossings, are found not to have the documents and entry visas required or who do not fulfil the conditions for entry to the territory laid down in Article 5 of the Schengen Convention of 19 June 1990. In the case of EU non-nationals applying at a consulate or at the border for a visa to stay in an EU

Member State, it also allows for fingerprints and photographs to be recorded, stored and electronically processed under the conditions laid down by the law of 6 January 1978.

Consulted by the Ministry of the Interior on certain articles of the draft law, in an opinion dated 24 April 2003, the CNIL pointed out, in particular, that — given the nature of the physical identification collected and the possible uses that might be made of the databases thus constituted — the storage and processing of fingerprint data were admissible only when justified by compelling reasons of public safety or public order. While thus underlining again its standard policy on the use of biometric techniques, the CNIL nonetheless stressed that it considered it legitimate to make use of biometric data recognition systems in order to establish a person's identity as long as these data were retained on a medium for the exclusive use of that person.

The CNIL also considered that, given the scale of the databases which might thereby be established, appropriate guarantees should be provided to ensure respect for individual rights and freedoms, in particular regarding access to such databases, duration of storage and updating of the data.

C. Major case-law

Failure, on the part of the Church of Scientology, to respect an individual's right to opposition

In 1997, when investigating a complaint by an individual who no longer wished to receive publications or letters seeking donations from associations linked to Scientology, the Spiritual Association of the Church of Scientology of Île-de-France had informed the CNIL that the personal data of the applicant had been removed from its files. However, in March and April 2000, that person again received various letters and publications from this association where the computerised address label bore the same identification number as three years previously. The CNIL referred this case against the Spiritual Association of the Church of Scientology of Île-de-France to the judicial authorities (Paris court) on 20 June 2000. On the strength of the facts, the Association was heavily fined in first instance (decision of 17 May 2002). The Court of Appeal, while it upheld the sentence in principle, reduced the fines imposed (decision of 13 October 2003). The applicants had subsequently introduced an appeal on a point of law.

Conviction of the controller of an anti-sect website for failure to notify the CNIL of the website

The controller of an anti-sect website had reproduced on the site two newspaper articles which mentioned the name of a person responsible for a company which was deemed to emanate from Scientology. The latter filed a complaint for failure to report automatic processing of personal data and for storing data linked to religious and philosophical opinions without the consent of the person concerned (Article 31 of the law of 1978). On the latter point, it was ruled that there was no case to answer; however, the Court sentenced the webmaster for failure to carry out the formalities prior to processing. The fact that the webmaster had notified the site from the onset of civil proceedings was considered to be irrelevant.

Rulings related to spamming

In one case, the Tribunal of First Instance of Draguignan handed down a ruling on 18 September 2003 sentencing the manager of a computer company for having used, on his office computer, software for the automatic collection of valid electronic addresses (direct e-mail collector), which he had intentionally connected to the message handling server used by the company Wanadoo Interactive, a subsidiary of France Télécom. To access these addresses which had been allocated, the defendant undertook a directory extraction comprising up to 23 million spammings or attacks on five machines of the e-mail server. The

Tribunal considered that the fact that the suspect had undertaken non-authorised extraction from a database belonging to a third party by using software which allowed him to obtain the file at minimum cost constituted the offence of unfair collection of personal data. The defendant has filed an appeal against this ruling.

In a second case, a judgment on spamming was delivered on 6 June 2003 by the Criminal Court of Paris. The ruling was delivered against a computer scientist who had engaged in spamming to promote a pornographic site. In handing down the sentence, the Court disregarded the argument of unfair collection of personal data through the delivery of unsolicited e-mails. However, it considered that the offence of failure to notify the CNIL prior to processing (prior formalities) was established and on this point a fine of EUR 3 000 was imposed.

Decision of the Council of State regarding access to the personal data contained in the Schengen information system (SIS) and in the files pertaining to State security, defence or public safety

At the end of 1995, while in transit at Roissy airport, the spiritual heads of a major sect were served with a decision prohibiting them from continuing their journey to Spain, owing to an SIS alert for the purposes of non-admission. Under Article 39 of the law of 6 January 1978, whereby persons have only an indirect right of access to their personal data contained in files concerned with the security of the State, defence, or public safety, a member of the CNIL was appointed to check, at the request of these two persons, the data concerning them in the SIS, so that these could be rectified or deleted as appropriate. The applicants considered that the alert relating to them was unlawfully based on their religious convictions alone, which could qualify them as coming under one of the categories of persons covered by the Schengen Convention. The checks carried out by the CNIL revealed that the applicants had indeed been alerted for the purposes of non-admission on the initiative of Germany 'owing to their membership of a sect likely to threaten public order'. The applicants were notified of these checks.

The applicants then brought an action in the Administrative Court, firstly for annulment of a tacit request for the application to be struck out arising from the silence of the Ministry of the Interior on their application to delete the data concerning them in the SIS, and, secondly, an appeal for annulment of the CNIL 'decision' whereby it had notified the applicants that it had undertaken the checks. The applicants had taken exception to the CNIL having rejected their additional applications for communication of the data.

In its ruling of 6 November 2002 on this matter, the Council of State, the supreme jurisdiction in administrative matters, delivered a judgment which reverses its previous position on the issue. Up to the present time, in order for requests for the release of information to be processed in accordance with the provisions of Article 39 of the law of 6 January 1978, it had deemed it sufficient that a file as a whole be relevant to State security, defence, or public safety. In its decision, on the contrary, the Council of State introduced the principle of the 'severability' of police files: 'where processing relates to State security, defence or public safety, it may encompass, on the one hand, data whose release to the data subject might be likely to undermine the purposes attributed to this processing and, on the other, data whose release would not undermine these same purposes, and in particular administrative or Court decisions which have been or should have been communicated to the data subject in advance'. Thus, the judge makes a distinction between the data contained in the police files. In the case of the former data, it is henceforth up to the CNIL, at the request of the data subject, to inform him/her that it has undertaken the necessary checks. In the case of the latter data, it will be up to the controller or the CNIL, at the request of the data subject, to release the data to him/her with, in the case of the CNIL, the agreement of the processing officer. The law of 18 March 2003 on internal security has taken account of this decision of the Council of State and has amended the wording of Article 39 of the law of 6 January 1978 accordingly.

D. Specific issues

Distance selling: storage and use of bank card numbers
Following wide consultation of the main professional federations and the competent authorities and a call for public contributions which received 2 300 replies from consumers, on 26 June 2003 the CNIL published a recommendation on the storage and retention of bank card numbers in the distance selling sector. In particular, the CNIL recommended that the use of the bank card number for purposes of commercial identification should, when this number is retained beyond the time necessary to conclude a transaction, require the consent of the person concerned.

The 'Spam box' initiative
On 10 July 2002, the CNIL announced the launch of the 'Spam box' initiative ('Boîte à spam'). Conducted over a period of three months, this campaign made it possible, by processing the more than 320 000 messages received, to obtain a precise overview of the phenomenon of unsolicited direct e-mail marketing in France, to report five originators to the Prosecution Service, and to propose a teaching module for web users entitled 'Halte au spam!' ('Stop spam!') on the CNIL website. The results were published on 21 November 2002 in a report *Spam box initiative: advice and action by the CNIL regarding unsolicited e-mail communications* ([4]).

In addition, on 4 November 2002, the CNIL forwarded to the Prosecution Service of the Paris Court of First Instance five deliberations reporting acts of spamming which it had adopted on 22 October 2002; one has given rise to criminal proceedings, whereas two cases have been dropped by the public prosecutor.

Electronic voting
In 2002 and 2003, the CNIL looked at several trials of electronic voting systems and concluded that the conditions for ensuring validity and security had still not been met. To this end, on 1 July 2003, the CNIL adopted a recommendation concerning the security of on-the-spot or distance electronic voting systems, particularly via the Internet. This included a number of strong recommendations designed to guarantee the anonymity and confidentiality of the vote as well as the transparency of the computer systems used (keeping the voter's personal data and the voting file on separate computer systems; encryption of the paperless voting card from the time it is issued on the terminal; encrypted files: encryption/decryption keys to be kept in sealed form, etc.).

Monitoring of diseases subject to mandatory reporting
In 2002, the CNIL authorised the epidemiological monitoring system covering diseases for which reporting is mandatory, including HIV/AIDS, set up by the National Health Monitoring Institute (Institut national de veille sanitaire). The CNIL oversaw work to ensure the total and irreversible anonymity of personal data (anonymity at the source of the declarations; computerised coding of the initials of surname and forename and date of birth; identification of subject's place of residence restricted to department code only; and profession recorded only as socio-professional category).

Geolocalisation of children
The development of services which use the geolocalisation data obtained when using a mobile phone to identify children's locations has led the CNIL to consider the conditions for using this type of service. As a basis for its study, it launched a call for public contributions to

([4]) The report is available on the CNIL website (http://www.cnil.fr/fileadmin/documents/approfondir/rapports/boite_a_spam.pdf).

which more than 1 600 persons replied in four months. The results of this study are available on the CNIL website ([5]).

CNIL report on blacklists

In a general report on 'blacklists' (November 2003), the CNIL pointed to the risks incurred by the increase in the number of such files and, since this practice is developing outside any specific legal framework, it wished to see more adherence to certain principles, outlined in this report: (i) 'blacklists' may not be secret; (ii) establishment of and access to the file must be limited to one sector and solely to professionals from that sector; (iii) strict adherence to the conditions for registration; (iv) guarantee of the right to erasure of data; (v) guarantee of the security and confidentiality of the data. This report is available online on the CNIL website in English and French.

Monitoring of new technologies

Throughout 2002 and 2003, the CNIL published several discussion documents designed to raise awareness among the public and industry of data protection issues in the context of certain technologies. The following topics were broached: Wi-Fi; the issue of TCPA (trusted computing platform alliance — proposal of the Trusted Computer Group); problems linked to 'messenger spam'; radio-frequency identification technologies (RFId); encryption; anonymisation; biometrics; wireless technologies; and a document on the Internet of the future and alternative technologies (PETs).

All these documents are available online on the CNIL website (http://www.cnil.fr).

E. Website

The new website of the CNIL has been online since 10 March 2004. Its main objective is to make the CNIL more accessible by providing clear and precise information to the public and by permitting users to interact more easily with the institution. On average, 127 000 visitors contact the site each month (102 000 unique visitors and 713 000 pages consulted).

Since August/September 2003, it has also been possible to subscribe to a monthly information letter edited by the CNIL Communications Service; after six months in operation, the letter already has 5 900 subscribers.

Germany

A. Legislative measures adopted under the first pillar

1. Act to modernise statutory health insurance of 14 November 2003. This act made major changes to healthcare in the statutory health insurance sector (health reform). Changes, sometimes considerable, were made to the data flows between the institutions involved. Doctors' invoices to statutory sickness insurance schemes are now done in respect of insured parties.

2. Act to incorporate social assistance law into the Social Security Code (SGB XII) of 27 December 2003. This introduced a major reform to social assistance legislation. The main feature was a new system for measuring rates and services. This basically took into account the requirements under data protection legislation concerning the procedures for comparing data.

3. Act on the Introduction of Federal Motorway Tolls for HGVs (Motorway Toll Act — ABMG) of 5 April 2002, which has been in force since 12 April 2002 (BGBl. I, p. 1234).

([5]) http://www.cnil.fr/index.php?id=1014.

The ABMG has paved the way for the distance-based levying of motorway tolls for heavy goods vehicles (HGVs) with a total weight of over 12 tonnes. Thanks to an electronic system, which is still being developed, the levying and billing of tolls should in future be largely automatic, allowing the current system of tolls based on time used (the HGV 'Eurovignette') to be discontinued.

4. Act on the Ongoing Development of Germany as a Financial Centre (fourth financial development law) of 21 June 2002, in force since 1 July 2002 (BGBl. I, p. 2010).

5. During its last term of office, the federal government set itself the target of developing Germany as a financial centre. This is particularly important for bolstering the confidence of domestic and foreign participants in financial transactions in Germany. The creation of mechanisms to better combat criminal operations in the financial sector is an important part of this plan. Provisions that make it easier to control money flows and check accounts are relevant in terms of data protection. Particular mention should be made here of the legal basis for the automatic consultation of account details pursuant to Section 24c of the Banking Act (KWG). Under the terms of this section, all credit institutions are obliged as from 1 April 2003 to keep a special file from which the competent authority can automatically download data in a manner stipulated by the authority in question.

6. Ordinance on Data Protection for the Provision of Postal Services by Businesses (Postal Services Data Protection Ordinance — PDSV) of 2 July 2002, which entered into force on 3 July 2002 (BGBl. I, p. 2494).

   The new PDSV incorporates the amendments to the postal law from the year 2001. It regulates the compilation and handling of personal data and thus the fundamental rights and obligations of those involved in postal services. It sets out particularly clear criteria for the disclosure of new forwarding addresses to other competitors. The new PDSV also takes account of technical progress, for example electronic signing for postal deliveries (hand scanners) or electronic tracking and tracing on the Internet.

B. Changes made under the second and third pillars

1. Law to combat international terrorism (Combating of Terrorism Act — TBK) of 9 January 2002 (BGBl. I, p. 361).

   The Combating of Terrorism Act amended a number of laws relating to domestic security (Federal Constitution Protection Act, Military Counter-Intelligence Service Act (MAD), Federal Information Service Act (BND), Article 10 Act, Security Clearance Check-up Act, Federal Border Police Act, Passport Act, Identity Cards Act, Act of Association, Federal Criminal Investigation Office Act, Foreign Nationals Act, Asylum Procedure Act, Act on the Central Register of Foreigners).

   Corrigendum of 7 August 2002 (BGBl. I, p. 3142).

2. Act on the Reorganisation of the Customs Investigation Service (ZFnrG) of 16 February 2002 (BGBl. I, p. 3202).

3. Act to step up the combating of money laundering and terror funding (Money Laundering Act) of 8 August 2002 (BGBl. I, p. 3105).

C. Major case-law

1. Decision of the Federal Social Court on the issue of hospital discharge reports (BSG of 23 July 2002 -3 KR 64/01 R-).
   In this judgment, the Court rules that statutory sickness insurance schemes may not *ipso jure* demand access to patients' records, but must bring in the medical service of sickness schemes in order to examine these.

2. Important decision of the Federal Administrative Court of 29 October 2003 concerning data collection from customers who use cellphones with prepaid cards. The existing regulation in the Telecommunications Act of 1996 does not commit the telecommunication providers to store the names and addresses of their clients. This is an important decision because the data protection authorities have always postulated that service options should be provided which allow anonymous access to publicly available telecommunications services.

D. Specific issues

1. Employee Data Protection Act: The *Bundestag* has repeatedly expressed the hope that the federal government would submit to Parliament a draft law to create a sector-specific employee data protection act. However, no such bill has yet been submitted. Given the increasing use of technology at the workplace and the possibilities this opens up of closely monitoring employees' performance and behaviour, there is an urgent need for such legal regulation.

2. The success of the complaint by the former Federal Chancellor, Helmut Kohl, at the court of highest instance against the publication — by the federal agency responsible for managing documents on the former German Democratic Republic (GDR) secret service — of files containing personal data on him, brought about an amendment to the Stasi Files Act which is ultimately justifiable from the point of view of data protection. Previously, the legal situation was that personal data on figures from contemporary history, politicians or holders of official functions could not be disclosed for, say, research purposes if the people in question had been victims of the secret services. The situation now is that case-by-case assessment will take place. It was only during the parliamentary procedure that an additional clause was included in the amended provision stating that such assessment should take into account whether or not the collection of information recognisably constituted a violation of human rights.

3. During the reporting period, a start was made on implementing the national visa information system.

E. Website

The website of the Federal Data Protection Commissioner (FDPC) is at www.datenschutz.bund.de or www.bfd.bund.de.

The website of the Virtual Privacy Office is at www.datenschutz.de.

Both sites are regularly updated. The FDPC site, for instance, has been expanded to include technical guidelines on data security in USB applications, the use of encryption procedures, data protection and telemedicine, data protection and Windows XP professional. Every two years, the latest FDPC activity report is put on the website and made available for downloading in PDF format. New versions of FDPC information brochures Nos 1 to 5 are also going ahead. The website also features the latest press releases and a complete overview of the findings and decisions of national and international data protection conferences.

The data protection profile (based on the common criteria) can also be downloaded for user-configurable information control. This profile is made up of requirements that protect an IT system's information flows for users in a transparent manner. To do this, the permissibility of an information flow is monitored according to clearly defined rules on data transfer. This security device is particularly useful for IT users who have limited IT expertise in ensuring data security but who are subject to security requirements concerning confidentiality, integrity and/or authenticity. Possible uses include e-commerce (data warehouses etc.), e-government (contract awards, application filing, etc.), health (electronic patient records etc.) and tele- and media services (teleworking etc.).

Greece

A. Legislative measures adopted under the first pillar

No major developments to be mentioned.

B. Changes made under the second and third pillars

The Hellenic Data Protection Authority, under its competence of N-SIS supervisory authority, addressed a letter (245/3-3-2003) to the Hellenic Sirene Office underlining that, according to Articles 109, paragraph 1, and 110 of the Schengen Convention, in combination with Articles 12 and 13 of Law 2472/97 on data protection, rights of access, correction and deletion must be addressed directly to the Sirene Office and that the latter cannot deny submission of such applications by anybody. In addition, the Sirene Office must provide every three months an analytical report on the number of people who have enacted their rights, the content of the applications and the time and content of the responses.

C. Major case-law

- Decision 77A/2002
  Reference to the religious beliefs of pupils on school certificates is illegal.

- Decision 86/2002
  The creation of a 'white list' by the Banks Information System Organisation Teiresias, created by the Union of Greek Banks for the protection of creditworthiness, is illegal unless there is the consent of the data subject.

- Directive 2/2003
  The transcription of Greek names into the Latin alphabet on identity cards and passports according to an automated letter-to-letter pattern model issued by the Ministry of the Interior should not prevent the holder from choosing the way his/her name should be written, such as how it was in previous national or foreign public documents or according to the way he/she participated or was known in social or economic life.

- Decision 52/2003
  The Athens Venizelos international airport pilot project to set up a passenger control system based on biometric methods (iris scans and fingerprints stored on a smart card) is in breach of the proportionality principle provided for under Directive 95/46/EC and therefore relevant permission was not issued.

D. Specific issues

- On 13 February 2003, the new President and the members of the Data Protection Authority were elected by Parliament, according to the procedure provided by Article 101A of the Constitution and Article 3, paragraph 2, of Law 3051/2002 (see below) on the constitutionally guaranteed independent authorities, for a four-year mandate. Mr Dimitrios Gourgourakis, Honorary Vice-President of the Supreme Court, was elected President.

- Pursuant to Articles 9A and 101A of the Constitution, adopted under the latest constitutional revision in 2001, according to which the right to the protection of personal data and the establishment of a relevant independent authority were incorporated into the Constitution, Law 3051/2002 (Official Gazette A220/20-9-2002) was adopted, regulating the function of the independent authority provided for in the Constitution.

- By Law 3115/2003 (Official Gazette A47/27-2-2003), the independent Authority for the Guarantee of Communications Secrecy was established, pursuant to Article 19, paragraph 2, of the Constitution.

E. Website

www.dpa.gr

Ireland

A. Legislative measures adopted under the first pillar

No major developments to be mentioned.

B. Changes made under the second and third pillars

No major changes made.

C. Major case-law

All decisions were decided on by the Data Protection Commissioner and no appeals were made to the courts against his findings as is provided under law.

D. Specific issues

Public awareness and national identifier

The detailed findings of a public awareness study carried out by the Commissioner's Office in 2002 revealed that people regarded protection of personal privacy as being very important. While 39 % of those surveyed were aware of his Office's role compared with 25 % in 1997, the Commissioner is not happy with this overall level of awareness. He also feared that the proposal to make the PPSN a unique health identifier number could be the start of 'function creep' and the creation of a national identity number by the 'back door'.

The year 2003 was extremely busy for the Commissioner's Office as new legislative provisions came into effect from July 2003 and business overall increased by, on average, 25 %. In this regard, guidance notes about minors and manual files were issued. He suspended judicial review proceedings begun in 2002 against the Minister for Justice pending the enactment at an early date of legislation regarding the retention of communication traffic data. In line with the enactment of new legislation, privacy audits and inspections were begun. It was necessary to prosecute two legal firms to make them fulfil their statutory registration

requirements with his Office. Although these were the first ever prosecutions taken by the Commissioner since the Office was established in 1989, further prosecutions will, if necessary, be taken in future against anyone who breaches the acts.

Complaints
As a general comment, most data controllers are aware of their responsibilities. However, the following were the major complaints which arose during 2002 and are referred to in the Commissioner's annual report for the year.

- Banks: The Commissioner was concerned that a prominent merchant bank was recording customer phone calls in a less than transparent manner while another major retail bank disclosed data relating to other account holders to a customer. In the latter case, the Commissioner was far from impressed with the bank's initial response to the customer and to his Office.
- *Gardai*: In response to an access request, the *Gardai* (police force) discovered that inappropriate and unnecessary personal data of a member of the public was recorded on the 'Pulse' system. He also investigated the concern of a journalist that the *Gardai* had accessed her mobile phone records without proper authority.
- Motor insurance: The Commissioner was not convinced that marital status was necessary information for companies in deciding whether to grant insurance. The practice ceased after his intervention.
- Department of Defence and army deafness claims: The method of release of compensation award details to the Department of Social and Family Affairs was in breach of the Data Protection Act. While the Commissioner is as anxious as anyone that anti-fraud measures are taken, nevertheless the government is not a universal data controller and has to respect laws. Otherwise, there would be no need for specific legislative measures introduced over many years to prevent 'Big Brother' situations.
- General election canvassing and other direct marketing methods: The Commissioner ruled that automated phone recorded messages delivered on the eve of the 2002 general election polling day was direct marketing and as such could only be made if prior consent was received. He also stopped other automated marketing SMS text and fax messages. The awareness study revealed that 60 % of people detest marketing phone calls.
- Chemists and infectious diseases: The Department of Health and Children withdrew a circular which required that chemists notify the health boards of prescription drugs issued to tuberculosis patients. While the Commissioner understands the importance from a public health perspective of having a reliable reporting system in place for infectious diseases, the law at present only requires doctors to so notify.
- Dublin Women's Mini Marathon: The organiser disclosed the database to a photographic company which put photographs on the Internet. Competitors could purchase their photographs but they were not made aware of this practice nor given an option to decline this service. The entry form has since been changed.

The following were the major complaints which arose during 2003.

- Freedom of information (FOI): The Commissioner stopped the Minister for Communications, Marine and Natural Resources from continuing to publish the personal details of people who made FOI requests to his department on the website as the Commissioner wanted to ensure that persons should be able to exercise their legal rights under freedom of information legislation without having to forgo their privacy rights.
- Hospital investigation: Patients were concerned that their medical records were sent for review without their consent. The Commissioner did not accept this as patient care and

future concerns made the actions appropriate. Similarly, a hospital was correct in seeking a review of a consultant's action without getting his prior consent or that of his patients. In that regard, data protection does not prevent appropriate remedies being taken especially in the medical area. In another complaint, a doctor acted properly in refusing access to a person's medical file.

- Baptism records of the Catholic Church: These are a statement of fact and need not be deleted when a person no longer wishes to be classed as a Catholic.
- SMS messages: The Commissioner ruled that unsolicited automated SMS marketing messages were wrong and any future such actions will be prosecuted by him in line with new regulations introduced in 2003 to combat spam.
- A head hunting employment firm was wrong to disclose one of its clients' details to his current employer.
- Marketing database caused minors to be marketed for a credit card: Due to an administrative error by a marketing company in compiling a marketing mailing list, minors were marketed for a credit card by a bank. The bank had rented the mailing list in good faith from the marketing company. The consent for minors has to be extremely high.

Enquiries and complaints
The number of enquiries received by the Commissioner's Office increased from 2 900 in 2001 to 3 200 in 2002, while the official data protection website (www.dataprotection.ie) recorded approximately 20 000 hits during the year. The most common specific queries related to the right to access personal data, the credit reference system, and direct marketing. The complexity of enquiries increased.

The number of formal complaints concluded in 2002 was 295 as against 171 in the previous year, with 189 new complaints being received (175 in 2001). Complaints mainly concerned organisations in central and local government (9 %), the direct marketing sector (10 %), public services (17 %), financial services (24 %), the telecommunications and IT sector (16 %), and the health and medical sector (7 %). The Commissioner indicated that 19 % of complaints were upheld and 37 % were not upheld, while 44 % were resolved informally.

In 2003, the Commissioner noted that the number of enquiries received by his Office was in the region of 10 000 which was a significant increase from previous years, while the official data protection website (see address above) recorded approximately 30 000 hits during the year. The most common specific queries related to general information, the right to access personal data, the credit reference system, direct marketing, and medical matters. The Commissioner noted that the complexity of enquiries was increasing.

The number of formal complaints concluded in 2003 was 199 while 258 new complaints were received (189 in 2002). Indeed, for 2004 some 110 have been received to March 2004. Complaints mainly concerned organisations in central and local government (9 %), the direct marketing sector (12 %), SMS (10 %), public services (15 %), financial services (14 %), the telecommunications and IT sector (9 %), and the health and medical sector (7 %). The Commissioner indicated that 20 % of complaints were upheld and 18 % were not upheld, while 62 % were resolved informally.

Registrations
While registrations with the Commissioner's Office rose in 2002 by 18 % to 3 632, he drew attention to a bogus registration company, which was issuing notices to companies. He referred the matter to the police for investigation.

In 2003, registrations with his Office rose by 28 % to 4 618 (fee income of EUR 455 000 compared with EUR 350 000 in 2002) due to a more proactive approach.

E. Website

www.dataprotection.ie

Italy

A. Legislative measures adopted under the first pillar

In the summer of 2002, an act was passed (Act No 189 of 30 July 2002) amending the legislation on immigration and asylum. This act, *inter alia*, requires that any foreigner applying for (renewal of) a residence permit is to have his/her fingerprints taken. The Garante pointed out — in a letter sent to the chairmen of both Houses of Parliament — that, in the light of the safeguards provided for at international level, it was necessary to comply with data protection principles with particular regard to collection, retention and subsequent use of such data. The Garante was also requested to give its opinion on the implementing regulations to be enacted with a view to both setting out the technical arrangements to take fingerprints and selecting the systems to be used in order to take and store the said fingerprints in the form of biometric data, which also entails the interconnection of different filing systems. In its opinion, the Garante referred to the document issued by the Working Party on the use of biometric data and stressed the need to comply with data protection principles, in particular with purpose specification and proportionality principles.

In 2002, Act No 222 of 9 October was also passed with a view to bringing to light unofficial employment.

In the course of the relevant legislative process, the Garante pointed out to the government that amendments were necessary, in particular with regard to two provisions of special interest in connection with the taking of fingerprints. Initially, the processing of personal data concerning non-EU residents, if acquired by means of fingerprint data, was to be regulated by the special provisions applying to processing operations by the Data Processing Centre of the Public Security Department. Furthermore, it was envisaged that fingerprints would be taken from all Italian citizens at the time of issuing their — yet to be precisely regulated — electronic ID cards. The Garante pointed out in its opinion that the provisions regulating the Data Processing Centre of the Public Security Department could not apply in full to the taking of non-EU residents' fingerprints, which was performed mainly for identification rather than for public security purposes. Secondly, we requested that a paragraph be added to specify that the envisaged taking of fingerprints from Italian citizens would in all cases be compliant with the data protection principles concerning use, storage and availability of the data.

The government undertook to submit a report to Parliament on the criteria that it plans to apply in order to implement the above provisions, in particular as for the taking of fingerprints.

Act No 3 of 16 January 2003 concerning organisational provisions with regard to the public administration envisages actions aimed at enhancing technological innovation in the public administration with particular regard to the national services card and computerised access to public administrative records. In this connection, it should be pointed out that the aforementioned act no longer refers to the electronic ID card, further to an amendment made by Parliament. This amendment was based on the need to prevent that such a sensitive issue, entailing control on personal data as well as requiring appropriate privacy safeguards, be regulated via instruments adopted exclusively by the government.

Important provisions applying to the processing of personal data in the employment context were adopted via a decree (Legislative Decree No 276 of 10 September 2003 on implementing the law-making power conferred on the government with regard to employment and labour markets as per Act No 30 of 14 February 2003). In particular, it was provided that the Garante would give appropriate guidance when issuing its opinions on the draft ministerial decrees where the mechanisms for data processing will have to be set out as also related to the information flows facilitating the confluence of employment demand and offer. Safeguards were expressly set out concerning the information to be provided to data subjects whenever job advertisements are published in newspapers or else via electronic communications networks (Section 9); furthermore, any discrimination possibly due to the processing of sensitive data and/or data that are irrelevant and excessive with regard to the purposes usually associated with the employment context were prohibited, which also applies to job agencies and any other entities able to perform personnel selection and surveys (Section 10).

Concern was raised, in particular, by a piece of legislation — Decree-Law No 269 of 30 September 2003, converted with amendments into Act No 326 of 24 November 2003 — setting out requirements to monitor healthcare expenditure. During the process leading to conversion of the decree-law, the Garante drew Parliament's attention to the sensitive issues raised by Section 50 of the decree-law — providing, *inter alia*, for the establishment of a database containing the fiscal identification codes of all healthcare beneficiaries in order to monitor healthcare expenditure. We pointed out that the purpose sought by the decree-law was undoubtedly in line with streamlining supervision over the State's expenditure; however, the tools envisaged to that end might jeopardise citizens' rights to the protection of their personal data — in particular, the data concerning health, which are covered by special safeguards. Indeed, it might always be possible to trace each data subject's medical history based on the information concerning prescriptions and specialists' advice. We pointed out that the legislation in force already envisages procedures to monitor healthcare expenditure without setting up centralised databases, and stressed that the need to increase effectiveness of such procedures should not result in limiting the right to personal data protection. In order to comply with personal data protection legislation, the monitoring system will have to require no processing of identification data; the setting-up of a centralised database, if any, should be based exclusively on the use of anonymised data.

B. Changes made under the second and third pillars

A decree (No 121 of 20 June 2002, converted into Act No 168 of 1 August 2002) concerning emergency legislation to ensure road traffic safety provides, *inter alia*, for 'distance' detection of speed-limit offences including, under certain conditions, the deployment of metering devices that may be used even in the absence of a police patrol. The Garante cooperated with the Ministry of Home Affairs in drafting an implementing instrument by setting out the required safeguards in respect of data protection issues.

Act No 88 of 24 April 2003, further to Decree No 28 of 24 February 2003, includes emergency legislation to fight hooliganism in connection with sports events. The Ministry of Home Affairs will have to lay down, jointly with the Ministry of Cultural Heritage and the Ministry of Innovation and Technologies, after consulting with the Garante, specific arrangements to implement the provisions regulating access to sports facilities. Such provisions basically consist of setting up access points equipped with metal detectors and supervised by law enforcement staff, where the entrance tickets will also be electronically scanned. Another decree by the Ministry of Home Affairs, again pursuant to the procedure described, will have to implement the provisions in the above act requiring that sports facilities be equipped with devices to allow filming and recording images of the areas reserved for the public both inside and outside such facilities, including nearby areas.

Act No 140 of 20 June 2003 contains provisions on interceptions and acquisition of reports concerning conversations and/or communications of Members of Parliament (MPs) as intercepted within the framework of judicial proceedings concerning third parties. This act provides, in particular, for the need to destroy reports and recordings concerning irrelevant interception activities (Section 6). The latter provision is related to general data protection principles, in that its violation may also entail the impossibility of using the personal data being processed — in accordance with Section 11 of the Data Protection Code.

C. Major case-law

Decisions by the Garante

During 2002 and 2003, there was a stepwise increase in the number of formal complaints lodged with the Garante — rising from 169 in 2001 to 608 in 2003. Quickness of the proceedings, reduced costs and high flexibility may partly account for the widespread use of this type of complaint with regard to a wide range of issues. Reference can be made here, *inter alia*, to the complaints lodged concerning data processing operations performed by the so-called private credit referencing agencies, in particular as regards data retention periods, those lodged in connection with processing operations carried out in the electronic communications sectors, many of them concerning spam, and those related to the insurance sector.

Very few provisions issued by the Garante further to complaint proceedings were challenged by the parties. A highly significant issue could be settled after the Garante's decision had been challenged before an ordinary court — namely, whether evaluation data should be considered to be personal data. The Garante's view was upheld by the court, recognising that data subjects may exercise access rights as well other rights set out in personal data protection legislation also with regard to evaluation data concerning them.

Case-law

In addition to the decisions made by the Garante on specific complaints, reference is to be made here to some important decisions issued by the last instance courts in Italy's judicial system, i.e. the Council of State and the Court of Cassation, concerning data protection.

The Council of State decided on an appellate proceeding concerning a judgment in which it was stated that the applicant's claim to get access to sensitive medical data was not so pressing and important as to override the data subject's right to privacy. The Council of State ruled that the data subject was not required to specifically give proof of an actual breach of his/her right to privacy, this right being protected as such with regard to data concerning health; conversely, the petitioner for access was to give proof of the 'importance' of the claim underlying his petition. If the data subject is not willing to consent to disclosure of the data concerning his/her health, the actual grounds he/she may adduce therefor are irrelevant because disclosure would as such jeopardise a good that is entitled to absolute protection — unless his/her claim is overridden by another claim that is entitled to equal protection (Decision No 2542/2002 of the Council of State, Division VI).

Another decision by the Council of State addressed the relationship between right of access and right to privacy, ruling that the laws in force do not provide general guidance on how to balance these two rights and actually allow an administrative body holding sensitive data to assess each specific situation on a concrete basis in order to decide whether access is necessary or not to establish or defend a claim that is at least equal to the data subject's claim to privacy (Decision No 4002/2003 of the Council of State, Division V). In another decision concerning this issue, the Council of State ruled that the right of access — albeit in its 'softened' version, i.e. as the right to inspect records — should override the right to privacy if

knowledge of the information is required to exercise the right of defence with regard to circumstances amounting to a criminal offence (Decision No 9276/2003, Division V).

As for the Court of Cassation, its Decision No 7341/2002 addressed the Garante's *locus standi* — an issue already mentioned in the sixth annual report — i.e. the possibility for the Garante to appear before courts and/or the Court of Cassation to defend the legal reasoning behind challenged provisions. The Court basically upheld the stance taken by the Garante and ruled that a petition filed with an ordinary court to challenge a provision issued by the Garante could not but be considered as the first instance judicial remedy available to the entity alleging damage as a result of the provision at stake. Therefore, the Garante is entitled to take part in a judicial proceeding related to the challenging of its own provision, irrespective of the proceeding of which the latter was the issue, in order to defend, in court, the same public interest that has prompted the Garante to act. In so doing, the Garante is bound to abide further by its impartiality obligations.

In two other decisions issued in 2003, the Court of Cassation ruled that non-pecuniary damage should be construed as a wide-ranging category including all cases in which there is violation of a value pertaining to human beings. Among the cases the Court considered to entitle to protection against the damage caused by the violation of individual-related interests devoid of pecuniary value, the use of unlawful means in collecting personal data was expressly mentioned (Decisions Nos 8827/2003 and 8828/2003).

D. Specific issues

Codes of conduct and professional practice

Special attention was paid by the Garante to the work in progress concerning several codes of conduct and professional practice as required by Section 20 of Legislative Decree No 467/2001. In addition to the code applying to processing of personal data for statistical and scientific research purposes in the public sector — which was published in the Official Journal on 1 October 2002 under the Garante's responsibility — reference should be made here to the work done concerning the codes on processing of data by private credit referencing agencies, private investigation agencies, and statistical and scientific research entities in the private sector; this work was basically concluded at the end of 2003, although the relevant instruments have yet to be published.

The code on the processing of personal data for statistical and scientific research purposes in the public sector was drafted in cooperation with the Garante by public and private entities representing the categories concerned. The provisions laid down in the code — which is to be abided by in order for the relevant processing operations to be lawful — apply to the processing carried out by statistical bodies and agencies taking part in implementing the national statistical programme.

The main features of this code are the safeguards to ensure anonymity of citizens, including the criteria to assess the identification risk related to the association between identification data and collected information as well as specific safeguards in respect of processing sensitive data.

The code also contains provisions requiring data subjects to be adequately informed as well as specific rules of conduct, and the security measures to be adopted with particular regard to the retention of identification data.

Employment context: collecting personal data via coupons and job advertisements
The Garante has repeatedly addressed the processing of personal data that are collected via coupons and/or job advertisements published in newspapers and journals. In particular, following several reports as well as the assessment carried out on a sample of job advertisements, the Garante issued a new provision of a general nature (provision of 10 January 2002).

Having established that several advertisements contained inadequate information and that the wording used to request consent to the processing of personal data was often generic and inappropriate, the Garante reaffirmed that respect for the fairness principle required applicants to be unambiguously informed at the time job advertisements were published on processing mechanisms and use of the personal data they were required to provide. In practice, each company should allow for the applicants' free informed choice and obtain, if necessary, their specific consent. The Garante also made available the text of a standard information notice to be possibly reproduced in job advertisements, including the use of standard wording.

Spamming
In 2002, the Garante blocked the processing of personal data stored in the databases of seven companies operating on the web. These companies acted in breach of the privacy law using e-mail addresses unlawfully, without the data subjects' informed consent, to send unsolicited commercial and promotional messages.

More recently, on 29 May 2003, the Garante adopted a general provision concerning unsolicited messages sent for direct marketing, advertising and promotional purposes. The opt-in principle was reaffirmed, by stating that e-mail addresses that are publicly available on the web, and on discussion groups' or on registrars' directories, are not to be used to send unsolicited messages, unless the addressee has given his/her prior consent and has been informed of the rights arising from the data protection law. Therefore, the Garante prohibited further unlawful data processing aimed either at sending advertisements or carrying out direct marketing activities, or performing market polls or interactive commercial communication.

In consideration of the transnational nature of the problem, the Garante has been actively taking part in international networks such as the CIRCA-based one, aimed at fostering cooperation between data protection authorities (DPAs) and dealing with international complaints.

MMS and data protection
Reports were submitted to the authority questioning compliance with personal data protection legislation of the use of the new mobile phones allowing images and sound to be rapidly recorded, stored and communicated to third parties by means of the multimedia messaging service (MMS).

These reports alleged that any person in the possession of a mobile phone capable of sending these messages could easily record and circulate images collected in public places, whether publicly accessible or not, in respect of individuals whose private sphere and dignity might be affected without their being aware of it.

The Garante clarified that the Data Protection Act did not apply if individual natural persons processed personal data 'for exclusively personal purposes' — for example, when a picture is taken and then sent to friends or relatives. Conversely, the act does apply if an image is collected and then disseminated on the Internet or else communicated to third parties on a systematic basis; as a consequence, the controller of the processing of the data contained in MMS messages is required to comply with all the relevant provisions on personal data protection.

Irrespective of whether or not the provisions of the Data Protection Act apply, any natural person sending MMS messages for exclusively personal purposes should comply with the obligation to secure the information collected. Furthermore, the Garante has stressed that the sender of such messages is liable to redress if damage (including non-pecuniary damage) is caused to third parties, unless he/she can prove that all suitable measures were taken to prevent such damage from occurring.

De-baptising
The Garante dealt, once again, with claims lodged by citizens requesting that their personal data as contained in the baptism registers kept in parish archives be modified on account of their having changed their religious orientations, alleging that their claims were grounded on their atheist beliefs.

The Garante stressed that it was impossible to delete the claimants' names from the relevant baptism registers, as the entries referred to an event that had taken place in reality; however, the claimants' request that their current religious orientations should be reported accurately was found to be justified. To that end, it was suggested that the baptism registers could be updated and supplemented by simply adding a rider to the information to be rectified.

Transborder data flows
Between the second half of 2002 and the first months of 2003, the Garante carried out a survey on a sample of companies, including the 50 biggest companies based in Italy, to assess what tools were implemented in order to transfer data abroad (SHA, standard contractual clauses, consent, contractual obligations, etc.). The findings of this survey showed that 5 of the 41 companies transferring data abroad made use of the SHA, i.e. 12.2 % of the total; 23 of 41 companies transferred data to the United States, therefore, 5 of 23, i.e. slightly more than 20 % of those in this group, implemented the SHA for their transfers. All of them had correctly notified the relevant countries of destination. Importantly, most companies availed themselves of the data subjects' consent to lawfully transfer the information.

As for the categories of transferred data, 35 companies transferred human resources (HR) data, 23 companies transferred customer-related data, 18 companies transferred data concerning suppliers and/or trade partners and 11 companies transferred other categories of personal data (obviously some companies specified more than one category of transferred data).

Multinational companies and transborder data flows
At the end of 2002, a draft project was submitted to the Garante envisaging implementation of a centralised information system at international level for managing a corporate group's human resources, to be outsourced to a US-based company. The above system would be managed with the support of entities located in several EU and non-EU Member States. The outsourcer and outsourcee had already entered into a so-called global agreement based on the standard contractual clauses for transborder data flows between data controllers.

The outsourcer company considered it appropriate — prior to implementing the project — to first consult some European supervisory authorities including the Garante. Taking account of the considerations made by this authority as well as by the other European supervisory authorities contacted, the company decided to revise the so-called global data transfer agreement previously made with its outsourcee and supplement it with or replace it by a new agreement, based mainly on the standard contractual clauses for transferring personal data to processors established in third countries. However, the clause concerning the data exporter's and importer's joint and several liability for damage caused to data subjects on account of the infringement of the rights and principles set out in the agreement was retained in the new version.

In the Garante's view, supplementing the controller-to-processor data transfer clauses by providing for the joint liability of both entities could result in a higher level of protection for data subjects' rights, as this approach could better ensure payment of damages, if any, to data subjects, who may take legal action directly against both contractual parties.

Furthermore, the Garante shared the corporate group's view that the draft agreement should be subsequently stipulated by each affiliate that had not conferred any specific mandate on and/or granted power of attorney to the holding company. Therefore, the Garante confirmed that the general authorisation concerning transborder data flows from Italy to processors established in third countries could apply to the data transfer at stake, and that there was no need for a new ad hoc authorisation.

Credit referencing agencies

The Garante has repeatedly addressed the processing of personal data by the so-called private credit referencing agencies (CRAs) as well as by banks and financial institutions accessing the relevant information systems, which include data on contractual and pre-contractual relationships in respect of the granting of credit, loans and/or mortgages with particular regard to consumer credit.

Ultimately, the Garante issued a general decision in July 2002 to provide guidance in this connection. The main features of this decision are the following.

(a) With regard to data quality, it should be carefully verified that the detailed data stored in information systems are relevant and not excessive. Defaulting should only be reported to a CRA if it concerns large sums and/or several instalments, or else if it is related to a marked delay; in any case, banks and financial companies should inform data subjects in advance so that the latter can take steps before their defaulting or another negative item of information is reported to a private CRA. Furthermore, data concerning credit applications should not be retained for longer than is necessary in connection with the preparatory activities prior to granting the credit.

(b) Proportionality is fundamental with regard to the retention of data concerning the relationships with the credit grantor(s). Accordingly, data concerning defaults that have been settled without losses, residual debts and/or unsolved claims are to be erased from the files held by private CRAs within one year either of the relevant settlement or, at all events, of the date on which the line of credit was extinguished. In addition, data concerning pending defaults should be kept for as long as the credit line is operating and, at all events, for no longer than three years after the date on which they had to be last updated by the CRA.

Furthermore, the companies managing and/or accessing private CRAs must carefully assess the criteria implemented and the checks aimed at ensuring that the information is correct and updated, and data subjects should also be granted access to the data stored in the form of a score concerning their reliability and/or creditworthiness.

Access to clinical records

In a decision of July 2003, the Garante specified the conditions to balance right to privacy and right to access clinical records held by healthcare institutions. This issue has been raised mostly in connection with the request made by defence counsels carrying out their own investigations to access records containing data on health and/or sex life. The principles referred to in this decision were subsequently supported by the provisions set out in the Data Protection Code.

In particular, the so-called 'equal importance' principle entails that processing personal data in order to enable access is only allowed if the right to be defended via the request for accessing administrative records is at least as important as the data subject's rights, or else consists in a personal right or another fundamental inviolable right or freedom.

Additionally, the Garante specified that the assessment of the claims at stake was to be carried out on a concrete basis by ensuring the data subject's appropriate information and participation. If the access request is granted only in part, it will be necessary to abide by data relevance and non-excessiveness principles.

Video surveillance
Many complaints, reports and claims were received by the Garante in 2002 and 2003 concerning the processing of data by means of video surveillance both in the public and in the private sector. In several decisions, it was stressed that the principles set out in a general provision issued in 2000 were to be abided by — namely, the obligation to provide an information notice, complying with the purpose specification and proportionality principles, ensuring that the processed data are accurate, relevant and not excessive, and limiting the data retention period. Additionally, many inspections carried out by the competent department at the Garante had to do with video surveillance. All the issues addressed will play a key role in contributing to the code of conduct that will specifically deal with processing operations carried out by means of video surveillance equipment.

Biometrics
During 2003, the Garante dealt with the use of biometric data by both private and public entities.

A project, 'S-Travel', envisaged initial tests at the Athens and Milan Malpensa airports on the use of biometric authentication technologies — based on fingerprints and/or iris scans — in the air transport sector with particular regard to check-in and boarding operations. The Garante pointed out that it was necessary to comply with data minimisation and proportionality principles as well as with data relevance and non-excessiveness requirements. In this case, the technologies to be implemented were only partly suitable for achieving enhanced security of airport controls. Furthermore, the collection of biometric data related to both fingerprints and iris scans of both eyes was found to be excessive and disproportionate compared with the purposes of the processing.

The Garante also took part in the activities of the Electronic Passport Working Party set up at the Ministry of Foreign Affairs in order to deal with the issues related to inclusion of biometric data in passports. The Garante's opinion was sought by the Ministry of Home Affairs in connection with the new electronic form to request residence permits.

Other initiatives
Memorandum of understanding with the finance police
In carrying out inspections, the Garante may avail itself, if necessary, of the cooperation of other State bodies, in particular police bodies. Therefore, the Garante and the finance police stipulated a memorandum of understanding with a view to enhancing supervision and control activities by means of increased cooperation between the two institutions.

Under this memorandum, the finance police will cooperate in the inspection activities carried out by the Garante — in particular by locating data and information on the entities to be inspected, allowing own staff to participate in the activities aimed at accessing databases and carrying out inspections, assessments and other investigations at the premises where processing operations are performed, providing assistance in all relationships with judicial authorities, performing activities under delegation of authority by the Garante in order to

detect breaches of criminal and/or administrative law, and carrying out surveys on the implementation of data protection legislation in specific sectors.

Outreach
Special care was taken in respect of communication activities. A weekly newsletter has been published since 1999 to provide the public with information on the Garante's activities. A CD-ROM containing a digital archive of these activities and the reference legislation — entitled *Citizens and the information society* — achieved its 10th edition in 2003.

Awareness-raising initiatives also include the organisation of meetings and workshops, publication of articles in newspapers, and participation in conferences and workshops throughout Italy. A front office operates daily (Monday to Friday).

In 2003, a television advertising campaign was carried out by means of a 20-second commercial broadcast by the public television channels.

The Garante's website was also enhanced. The new structure ensures its fully-fledged usability, implementing new advanced search tools to retrieve legislation and decisions.

E. Website

www.garanteprivacy.it

Luxembourg

A. Legislative measures adopted under the first pillar

Law of 11 November 2003 regarding the public register of real estate
The Commission nationale pour la protection des données (CNPD) expressed its concern about the use of the same national identification number as those used for internal purposes by other public administrations and until now kept confidential.

Law of 8 June 2004 regarding freedom of expression in the media
The CNPD was officially consulted about the documents submitted to Parliament and made its position public regarding specifically the exemptions and derogations from the provisions of the data protection law for data controllers carrying out processing of personal data for journalistic purposes.

The question of the need for fair information to be provided to the data subject on the purpose of the processing was raised by the national DPA in case the data are collected directly from the data subject.

B. Changes made under the second and third pillars

Law of 2 August 2002 regarding the driving rules on public roads
The institution of a driver's licence with a number of points deductible in case of major offences to the traffic code has led to specific regulations (secondary law) regarding the processing of personal data related to offences to the legislation concerning circulation on public roads by the police and by public administration. Data protection aspects have been examined by the CNPD.

C. Major case-law

Two court decisions of the Appeal Court concern questions of data protection and labour law. Both have been published before the entry into force of the law of 2 August 2002 regarding the protection of persons with regard to the processing of personal data. It is acceptable for an employer to supervise the activity of his/her employees at their workplace by means of a monitoring device.

In the present case, it is all the more justified as there has not been continuous control of the employees but the employer having serious doubts concerning the honesty of one of his employees punctually and exceptionally checked upon the latter.

The employee could not have overlooked the existence and position of the surveillance device, which is common in supermarkets.

Having knowledge of both the existence and location of the camera, the employee should have known that, in the circumstances, it was likely to occasionally film him during his worktime.

(Court of Appeal, 16 May 2002, Decision No 25801)

The Court assents to the case-law according to which tape recordings taken without knowledge of one of the parties are not a valid way of giving evidence.

Indeed, such recordings are obtained in an underhand and therefore irregular manner.

(Court of Appeal, 4 October 2002, Decision No 25235)

The first decisions taking into account the implementation in national law of Directive 95/46/EC are expected during the next few months.

D. Specific issues

Between 1 December 2002 (the date of entry into force of the new law) and 11 August 2003 (the deadline for the notification of data processing to the DPA), the CNPD had to deal with administrative, procedural and practical problems linked to the notification obligation set out by the law.

Much effort was put into providing information, explanations and guidance to business operators, public administrations, health organisations and other data controllers that have to comply with the new provisions.

Simplified models for notification have been prepared for standard data processing, which are unlikely to adversely affect the rights and freedoms of data subjects.

All forms and explanatory notes have been made available electronically (either via the website or on CD-ROM).

E. Website

The website of the Commission nationale pour la protection des données in French and German (www.cnpd.lu) was put online on 11 December 2002 during the first press conference of the CNPD.

Netherlands

A. Legislative measures adopted under the first pillar

No major developments to be mentioned.

B. Changes made under the second and third pillars

The government has prepared a proposal for the *Wet politiegegevens* (Data Protection (Police Data) Act), a renewal of the *Wet politieregisters* (Wpolr — Data Protection (Police Files) Act), which dated from 21 June 1990. Early in 2004, the legislative proposal was presented to Parliament, and to the Dutch Data Protection Authority (DPA) for advice. The proposal no longer provides for a duty to lay down a regulation for each police register, as is the case in the current Data Protection (Police Files) Act. Also, all data collected will be available to the whole police force during the first year, after which specific authorisations will be applicable. Furthermore, the proposal allows for an extension of the possibilities of exchange of personal data within the police force.

An act implementing a general identification duty has been proposed to Parliament. Upon the presentation of the proposal to the Dutch DPA, the Dutch DPA advised the Minister for Justice early in 2003 against bringing such a bill before Parliament. The proposed legislation failed to strike an appropriate balance between rights and obligations of the individual and those of the government. A permanent obligation would be placed upon the citizen without any evidence that specific obligations are not sufficient. Criminalising failure to identify oneself would create a situation in which any member of the public would be liable to be regarded as a suspect. The question of whether a limited or general obligation to identify oneself should be introduced has been debated in the Netherlands for the last 20 years. Hitherto, it has always been concluded that a general requirement would be unduly onerous. Given that the proposal was not based on fresh arguments in this regard, its implementation would constitute a contravention of the European Convention on Human Rights, which requires that any infringement of individual privacy must be adequately justified. In September 2003, a renewed proposal was presented to Parliament. In the updated proposal, that referred to the advice of the DPA, the age limit was raised from 12 to 14 years, and provided some more argument for the need for the identification duty. Moreover, the proposal no longer gave the police independent powers to check whether individuals carry an identification card; checks can only be done if necessary for the performance of the police task. The bill was under discussion in the Upper House early in 2004.

The Dutch Government tabled a proposal extending the powers of police and justice authorities to demand personal data from businesses and other organisations, in so far as necessary for investigation purposes. The proposal takes a layered approach with regard to the kinds of data that can be demanded. To this end, certain general powers of police and justice authorities will be taken up in the Code of Criminal Procedure. The Dutch DPA agreed with the Minister for Justice on the main lines of the proposal; it, however, stated that such considerable extension of powers demands that adequate structural safeguards are provided. It deemed necessary at least two structural safeguards: firstly, the possibility of a preceding review by the court of a demand for information, and, secondly, a systematic and regular inspection of the processing of personal data in the police files.

C. Major case-law

Bureau X

In 2002, the Dutch Data Protection Authority started a very thorough investigation into the operations of Bureau X. This bureau conducted financial investigations into natural persons, which is, in itself, common procedure in the Netherlands. In this case, however, the

information included not only facts that seemed inappropriate for that purpose but also facts that seemingly came from illegal sources.

After a 'paper investigation', an on-the-spot check was conducted. Due to the results of these investigations, the Dutch DPA decided to follow two strategies.

- A formal complaint was filed with the public prosecutor on suspicion of fraud, enticing breach of secrecy and non-notification of the Dutch DPA. In 2003, a third party, who was employed by the bureau to obtain information by assuming false identities, was sentenced to 12 months' imprisonment (six months provisional) and the bureau's own staff to alternative punishments. The director of the bureau still has to stand trial in 2004.
- The second strategy consisted of threatening Bureau X with financial consequences (an injunction to cease or duty backed by an obligation) if specified proceedings were not adjusted to the satisfaction of the Dutch DPA and in accordance with the Data Protection Act. According to the bureau, the duty backed by an obligation was not clear enough. The bureau went to court to appeal the duty backed by an obligation. According to the judge, the duty backed by an obligation was clear enough for Bureau X on how they should comply with the Data Protection Act. Appeal against the decision was still open for Bureau X early in 2004.

Dutch Association for Trade Information Agencies (Nederlandse Vereniging van Handels-informatiebureaus)
In 2000, the Dutch DPA conducted an investigation into the activities of a trade information company. The name of the company was not made public by the Dutch DPA. The Dutch Association for Trade Information Agencies demanded that the name of the company be revealed to it, since the company was a member of the Association. The Dutch DPA refused to make the name public with regard to the *Wet openbaarheid van bestuur* (Freedom of Information Act) because of the possible economic and financial harm for the company concerned. According to the Council of State (the highest court in administrative law in the Netherlands), the Dutch DPA could indeed have made the decision to keep the name of the company secret due to the possibility of economic and financial harm.

D. Specific issues

Reaction of the Dutch DPA to increasing focus on security
Security has been the primary focus of political and public debate over the last few years. The Dutch DPA sent a clear message that it is very concerned that a simplistic introduction of greater police powers could seriously undermine the rights and interests of ordinary citizens. It also publicly refuted the notion that privacy protection acts as a barrier to the resolution of social problems by hindering cooperation between various authorities. It is the Dutch DPA's conviction, borne out by experience, that privacy protection is one of the success factors for effective government. There are very few legitimate government objectives whose realisation may be impeded by privacy rules. Provided, that is, that such rules are taken into account from the outset in the design of organisational structures, information systems and procedures, and the formulation of policy. Reflecting on the purpose, necessity and scale of monitoring measures to be taken is imperative. Measures could also be temporary; their scope can be limited to places or times where there is increased risk. Evaluating the measures should be standard practice, certainly in the case of radical monitoring means such as surveillance cameras, preventive searching and identity checks. Well-thought-out measures, their proportional use and measuring their efficacy in combating terrorism and other forms of serious crime are part and parcel of a government that protects constitutional rights. In several pieces of (legislative) advice to the government, the Dutch DPA pointed to these principles.

Lack of respect for the privacy of the individual ultimately erodes public faith in the government. Citizens who have nothing to hide deserve a government that consistently takes privacy protection into account when formulating policy, designing information systems or defining the responsibilities of the individual. Hence, the right to privacy is fundamental to the security that a democratic constitutional State affords its citizens.

Social security investigation and fraud teams

Efforts to combat social security fraud received a lot of attention in 2002 and 2003. A variety of organisations are involved in the investigation of such fraud: (municipal) social security investigation teams, *regionale interdisciplinaire fraudeteams* (regional interdisciplinary fraud (RIF) teams) and the Sociale Inlichtingen- en Opsporingsdienst (SIOD — Social Security Investigation and Detection Service). Having been notified of certain data processing operations, the Dutch DPA carried out a prior check to assess whether the activities were organised on a lawful basis. Similar checks were initiated in the investigative activities of the Uitvoeringsinstituut Werknemersverzekeringen (Employee Insurance Scheme Executive Body) and the Sociale Verzekeringsbank (Social Insurance Bank).

The Dutch DPA assessed the process definition for covert observation drawn up by one of the RIF teams, as well as the associated working practices. In principle, the process definition was considered to provide adequate safeguards for the lawful processing of personal data. It was agreed that the process definition would be made available to other RIF teams by way of example. A similar approach was taken by the Dutch DPA in relation to (municipal) social security investigation teams.

It is hoped that the strategy adopted can lead to general nationwide harmonisation of the covert observation practices used by RIF teams and (municipal) social security investigation teams. This will be beneficial in terms of legal clarity and compliance with the Data Protection Act, while also simplifying the necessary notification of data processing activities.

Codes of conduct

In 2002, the *Gedragscode van de Nederlandse Vereniging van de Research-georiënteerde Farmaceutische Industrie* (code of conduct of the Netherlands Association of Research-oriented Pharmaceutical Companies) became the first code of conduct to be formally approved under the Data Protection Act. To secure approval, a code of conduct needs to reflect the provisions of the act and any other sector-specific rules governing the processing of personal data. Detailed discussions were also held with the banks and insurance companies in 2002 regarding the introduction of a similar code. The *Gedragscode verwerking persoonsgegevens financiële instellingen* (code of conduct for the processing of personal data by financial institutions) was ultimately approved in January 2003. The Dutch DPA regards the introduction of this code as a significant development.

The *Privacygedragscode sector particuliere onderzoeksbureaus* (privacy code of conduct for private investigation agencies) approved at the beginning of 2004 was drafted by the Vereniging van particuliere Beveiligingsbureaus (VPB — Association of Private Security Agencies) and binds the agencies affiliated to the VPB. Private investigation is a sector experiencing exponential growth, and one in which little was regulated. In the context of licensing these agencies, the Minister for Justice is planning to obligate all private investigation firms to comply with this code of conduct. The Minister for Justice and the Dutch DPA have concluded an agreement to coordinate supervision of the branch.

The code of conduct for processing personal data of the Nederlandse Vereniging van Handelsinformatiebureaus (NVH — Netherlands Association of Trade Information Agencies) was also approved. In this sector, in particular, over the last few years, the Dutch DPA has been forced to conclude that personal data protection has not been properly observed on a

large scale. The Dutch DPA will maintain the code of conduct of the NVH as a guideline in supervising all trade information bureaus.

Municipalities: notification and camera surveillance
For the citizen, the municipality is an important area of government with which he/she will be greatly involved. As a result, municipalities process great quantities of citizens' personal data. Because of developments in the duties and administration of the municipality, responsibility for protecting personal data is increasing. Consequently, it is crucial that municipalities have their information systems well organised, also with a view to protecting the personal data of their citizens.

An analysis of the first 13 000 notifications of processing personal data under the Data Protection Act showed that the number of notifications from municipalities greatly lagged behind expectations; at least 60 municipalities appeared to consistently ignore their obligation to notify. In a random check, the Dutch DPA then assessed a number of municipalities to see whether they had complied with the obligation to notify. In December 2003, the first municipality was penalised for failing to comply with this obligation.

In 2003, the Dutch DPA commissioned a survey into the use of camera surveillance by municipalities. The goal of the survey 'Camera surveillance in de openbare ruimte' ('Camera surveillance of public places') was to gain an overview of the way in which CCTV surveillance functions in practice and how the various municipalities address the privacy aspects of camera surveillance. The survey showed that one in five municipalities deploys such surveillance as a means of furthering security, public order and supervision. Over half of the municipalities that make use of CCTV, however, have not reviewed its effectiveness. Around half of the municipalities use camera surveillance in the context of cooperation between institutions and organisations. This generally involves cooperation with the police in tracking down criminals, although cooperating with companies and other organisations is also a regular occurrence. The frameworks within which this takes place, however, often seem unclear.

Certification of data processing
In various countries, a search is being conducted into ways of utilising competition and market mechanisms for privacy protection. One of the options of making it clear in the market that companies and organisations endeavour to handle personal data with due respect and care is a privacy certificate. Together with the Dutch DPA, a number of regulatory bodies have developed a system for the private auditing of processing personal data. The privacy certificate in mind can be allocated to a specific, legitimate processing of personal data. The certificate is thus not awarded to an organisation in its entirety. In the first instance, the Dutch DPA will appoint two accreditation bodies, the NOREA and the NIVRA, for the accreditation of privacy auditors. The system will gain practical form in 2004.

E. Website

All relevant information in Dutch can be found at www.cbpweb.nl. Information in English is available via www.dutchDPA.nl.

Portugal

A. Legislative measures adopted under the first pillar

- Legislative authorisation from Parliament for the interconnection of data between tax authorities and social welfare authorities.
- Decree-law, providing all credit institutions access to the central bank database on bold cheques.
- Law 99/2003 of 27 August 2003 — approves the Labour Code.

B. Changes made under the second and third pillars

Act 36/2003 of 22 August 2003 establishing rules for the implementation of Eurojust Decision 2002/187/JHA.

C. Major case-law

The Constitutional Court issued, during this period, two main decisions regarding data protection matters. The first is dated from June 2002 and concerns the use of video surveillance by private security agents for the protection of people and goods and also as a tool for self-protection. The Constitutional Court considered video surveillance to be part of the intimacy of private life, therefore integrating fundamental rights. So, the Court decided that only Parliament can approve legislation on video surveillance, and found unconstitutional a decree-law approved by the government.

The second decision concerns the Labour Code and includes data protection aspects. The Court found unconstitutional the possibility of the employer having access to information concerning health or pregnancy of the employee or during the recruitment process. The Court considered this to be disproportional and violating privacy. In the same way, the Constitutional Court considered that the health tests, mandatory by law for the purpose of medicine within the workplace, shall be restricted to the essential.

In 2002, following an appeal, the Central Administrative Court decided in favour of a DPA decision, which did not grant authorisation to the Chemistries National Association to centralise personal data, collected by its associates, on medicine prescription, list of prescribing doctors, special diseases, and much other sensitive information. The Court has made an interesting interpretation of the Data Protection Act, in particular on what sensitive data are concerned.

Also in 2002, the Central Administrative Court kept the DPA decision, which had ordered the deletion of data collected massively in the Car Register by an economic information company. The Court made interesting considerations on the use of data included in public registers.

D. Specific issues

- Processing of data in manual files: The DPA issued some guidance regarding the processing of data contained in manual files, once the data protection regime also applies to this kind of data. The Data Protection Act foresees a transitory period for the notification of manual files, and the DPA adopted special measures for sensitive data, whose processing has been initiated after the entry into force of the act.
- Employees' monitoring in the workplace: The DPA set some guidelines concerning the control of phone calls, e-mails and Internet access of employees. Whenever the employer intends to make such control, the processing has to be notified to the DPA and the employees have to be fully informed.

- Processing of sensitive data for reality shows: The DPA decided that the data subject has to provide express consent and the data controller has to delete the data immediately after the candidates for the show are chosen.
- Communication of data from the electoral enrolment database for political campaigns: The DPA only authorised the communication of this data concerning citizens living abroad for the purpose of political campaigns during the pre-election period. The DPA considered that this was a relevant public interest in this case. The data communicated are name and address and the data have to be deleted after the elections. The data subject has to be fully informed, in particular where the data were collected, and has the right to opt out.

Main opinions given by the DPA on draft bills

- Transposition of Directive 2000/26/EC.
- Access by all credit institutions to information held by the central bank on risky users of cheques.
- Rules concerning personal data processing within government-subsidised loan to buy a house.
- Creation of a list for public employment.
- Registration of religious legal entities.
- Personal genetic information.
- Courts and public prosecutors' databases.
- Patient Rights Charter.
- Labour Code — among other issues, the DPA considered unacceptable the use of genetic tests for staff recruitment.
- Criminal police access to civil identification national registration.
- Collection of electronic digital evidence — the DPA considered that either traffic data or the content of the messages could only be known by law enforcement authorities whenever there was a judicial mandate.
- EU recommendation on the localisation of people through emergency calls.
- Transposition of Directive 2001/50/EC.
- Transposition of Directives 2000/31/EC and 2002/58/EC.
- Creation of a database on minor illegal immigrants for the purpose of healthcare and education — the DPA considered that this database should not be held by the Internal Affairs Ministry.
- Regulation on the VIS.

E. Website

http://www.cnpd.pt

In 2003, the DPA started to draw up a new web page, including texts in English and French. There will also be a newsletter, though only in Portuguese for the time being. The new page will be online in 2004.

Spain

Participation in legislative developments constitutes a very important part of the Spanish Data Protection Agency's activity. According to the provisions of the organic law on data protection (Section 37h), the Agency is responsible, in mandatory fashion, for reporting on planned general dispositions that develop the law and any other draft legislation — law or regulations for interpreting a law — that have an influence on this subject. Throughout 2002 and 2003, a total of 66 dispositions were submitted for the Agency's consideration.

A. Legislative measures adopted under the first pillar

Directive 2000/31/EC on information society services and electronic commerce

On 12 July 2002, the law on information society services and electronic commerce (Lissec), which incorporates into national law Directive 2000/31/EC, was approved. The purpose of the new law is to establish an adequate legal framework for the provision of these services and thus to generate confidence among all participants in this sphere. We can underline the following aspects.

Scope: It applies to service providers (or intermediaries) established in Spain, i.e. those who manage their economic activity from Spain and to providers who are not resident or domiciled in Spain but who provide services through a permanent establishment in Spain (e.g. a branch office), although it will apply only to the services provided through that permanent establishment.

Retention of traffic data (for the purposes of their use in a criminal investigation, public security or national defence): Intermediary service providers also have the specific obligation of storing the data from traffic (only those needed to find the terminal used when transmitting the information) relating to electronic communications or to the origin of hosted data for a maximum period of 12 months for the purposes of their use in a criminal investigation or to safeguard public security or national defence. This obligation is without prejudice to the right of secrecy of telecommunications and data protection. It must be said that this obligation is not yet in force since secondary legislation must be passed establishing the specific categories of data to be kept, the different retention periods, the conditions of storage, the specific way in which the information shall be made available to the competent authorities, and the provisions for its destruction when no longer needed (Article 12).

Spamming: Commercial communications must be clearly identifiable, as well as the person that sends them, and the word 'publicidad' ('advertising') must always appear when they are sent using electronic mail. In any case, Lissec prohibits sending these commercial communications unless they are previously requested or expressly authorised by the recipients (Article 21).

Electronic commerce: This law recognises the complete validity and efficacy of electronically concluded contracts, comparing them to written contracts, without any agreement between the parties for the use of electronic facilities being necessary. In addition, it creates rights for users to receive prior information about the contract, the conditions applicable to it and the procedure that they need to follow to order, as well as a right to receive confirmation of the conclusion of the contract when the contracting process is complete. These information obligations can be bypassed only when none of the parties is a consumer and all parties consent or when the contract is concluded exclusively by exchange of e-mails (Article 23).

Data protection: The obligations affecting controllers in data protection matters have not been modified. These include the requirement of notification — of all processing operations — to the Data Protection Agency (DPA); and also the legal obligation to inform the subject in a transparent way about the purposes of the processing, and the recipients. Likewise, the new law does not affect the supervising and inspection competence of the Spanish DPA (Article 35.3).

Norms of nationwide application

Laws and development regulations directly affecting data protection
In addition to Lissec, the Spanish Data Protection Agency reported during 2002 on legislation with undoubted repercussions in the sphere of personal privacy and the protection of personal data, among which can be cited Law 41/2002 of 14 November 2002 basically regulating the patient's autonomy as well as rights and obligations regarding medical information and documentation, Law 44/2002 governing reform measures of the financial system, and Law 48/2002 of 23 December 2002 governing property tax registers.

The Agency has also examined the drafts of important development norms (secondary legislation) affecting this matter, among which we would highlight the royal decree through which the citizen's time of access to the services of the National Health System is guaranteed, the royal decree for the promotion of electronic administration, the regulations for interpreting Organic Law 5/2000 governing the criminal liability of minors, the royal decree that approves the regulations governing the General Intellectual Property Register, and the royal decree that lays down the procedures and technical measures for legal interception of telecommunications that can be demanded of telecommunications services operators available to both the public and public telecommunications networks.

Data protection aspects of the registration of Internet domain names
The national plan for Internet domain names under the '.es' country code for Spain was approved in March 2003. The plan came into effect one month after its publication, i.e. on 26 April 2003. This plan was already contemplated in the Information Society Services and Electronic Commerce Act 34/2002 of 11 July 2002 and, together with the act, seeks to lay down a framework for implementing the system of '.es' country code domain names.

The preamble to the order itself defines the Internet domain name system as a key operational aspect of the Internet, because single syllable suffixes are assigned to each system logged onto the Internet, thus facilitating their location and use on the Internet.

According to this new legislation, the function of the name assignation authority is to manage the register of domain names and data files required for making the Internet domain name system work. The Entidad Pública Empresarial Red.es is the public authority responsible for this task. We have initiated contact with Red.es in order to ensure compliance with data protection rights where management of this public register and the personal data included in it are concerned.

The new legislation seeks to combine standards such as reliability and flexibility. In general, domain name registration will be provided on a 'first come, first served' basis, provided that all the other requirements provided for in the plan are met.

In addition to restating the requirements for having access to and registering '.es' domains, repealing the order of 21 March 2000, the new order introduces major novelties into the domain name system.

(a) The first novelty in the plan is to reduce the restrictions applicable to the assignment of domains that had made the system one of the world's most inaccessible and restrictive (and hence one of the safest). The restrictions affecting geographical terms are lessened

and the entitlement to and type of domain names that may be applied for are broadened, although it is still necessary for the applicant to prove title to a name, trade mark or designation matching the domain name. This makes the system very secure and ensures compliance with industrial property rights.

(b) Furthermore, the plan makes provision for the creation of new third-level domains that will enhance the possibilities of assigning '.es' domains. These new domains are: '.com.es', '.nom.es', '.org.es', '.gob.es' and '.edu.es'; the first three will be assigned almost without restrictions, whereas the assignment of the last two will be conditional on evidence of satisfying certain requirements.

In order to protect the rights of the current proprietors of '.es' domains in so far as they may be affected by the new domains, a 20-day period will be given for the pre-emptive registration of the '.com.es', '.nom.es' and '.org.es' domains. There will also be a pre-emptive 20-day period for those satisfying the requirements for registering the '.es' domains because, after these periods expire, access to third-level domains will be almost unrestricted.

When the 'grace period' is over, any individual or organisation may contest applications for the new domains if they feel aggrieved and where it is deemed that they do not satisfy the requirements in place.

The said period has not yet begun because it will be the responsibility of the public commercial entity Red.es to determine the dates from which the periods shall start to run.

Those entitled to apply for third-level domain names are:

- '.com.es': natural or legal persons having interests in or related to Spain;
- '.nom.es': natural persons having interests in or related to Spain;
- '.org.es': non-profit entities, institutions or groups with or without legal personality having interests in or related to Spain;
- '.gob.es': Spanish public administrations and their dependent public law entities and any of their departments, bodies or units;
- '.edu.es': officially recognised entities, institutions or groups with or without legal personality carrying on teaching or research-related functions or activities in Spain.

(c) The third relevant novelty of the new plan is that provision is made for the creation of the figure of domain name registration agents who shall broker between the interested party and the registration body. In any event, interested parties may address their applications directly to the assignation body.

The public commercial entity Red.es will define the requirements to become a registration agent in the near future.

(d) Finally, the plan contemplates a bidding procedure for domain names with a special market value (those consisting exclusively of generic terms and those matching the names of Internet protocols, applications and terminology).

The new plan replaces former regulations and is forward looking, extending the possibility of access to the '.es' country code to all those with interests in Spain.

E-government

New regulation on electronic registers and information exchange within public authority offices (Royal Decree 209/2003 of 21 February 2003 — Official State Bulletin, 28 February 2003)

This comprises secondary legislation within a general framework for fostering the general State administration's use of electronic means. The purpose of this new regulation, approved by the Cabinet meeting last 28 February, is to:

- establish a new system of electronic notification requiring the citizen's prior consent to be notified by electronic means — expressed through an application form;

- facilitate the exchange of electronic information already available in public registers so as to make citizens' access to public services easier, by avoiding asking them for documents and certificates that must be issued by other public administration bodies.

This regulation fully complies with the Spanish data protection law (Law 15/1999 of 13 December 1999 (available in English at https://www.agpd.es/index.php?idSeccion=347) in two important aspects in particular.

First, because it ensures the safe transmission and reception of electronic notifications. To achieve this, a registration process must be followed. When registration is complete, the administration will provide the user with a single electronic address for sending and receiving forms and notifications, such as tax returns, VAT returns, etc. Forms can be sent using appropriate government websites, portals or third-party software packages.

In order to access this single electronic address, it will be necessary to provide a user name, password, and authentication mechanism solely for the purpose of these notifications, to guarantee their confidentiality. The application of authentication and encoding mechanisms to such communications is also being contemplated.

The second aspect related to data protection is the electronic transfer of data: certificates issued by a public authority office at the request of another public authority office and the transmission of data between public administrations. In this case also, the public administration needs the subject's prior consent for the data to be transferred.

(See the full text of this new regulation at http://www.boe.es/boe/dias/2003-02-28/seccion1.html#00000.)

Dispositions regulating electronic files that contain data of a personal nature handled by various entities

The number of norms aimed at the creation of files or the modification of already existing regulations that govern them has been particularly important among the draft general dispositions on which the Agency reported in 2002, particularly so in the sphere of the State's general administration. In 2002, the public files corresponding to the Ministries of Education and Culture, Development, Justice, Environment, Health and Consumer Affairs, and the Directorate-General of Police were regulated.

Analysis of this information leads us to conclude that the number of changes has been due, on the one hand, to the fact that the bodies responsible for the files were obliged to adapt their dispositions to Law 15/1999 (which established a transitory period of three years to bring into line the electronic files that pre-existed before the law came into force), and, on the other hand, to the need to incorporate the modifications into the said law introduced by the judgment of the Constitutional Tribunal 292/2000 of 30 November 2000 (which ruled that the law was partially contrary to the Constitution specifically in precepts related to public files, as we analysed in depth in our report of 2000, to which we refer you).

Another contributory factor has undoubtedly been the demand made by the Agency's Director on the ministerial departments and public bodies in previous years requiring them to regularise their situation.

Among the projects for general dispositions reported in 2003, there has been a significant number concerning norms directed at the creation of files or modifying the existing dispositions that regulated them. In 2003, the Spanish Agency reported on, among others, the draft order creating the National Register of Implants, the draft order of the Ministry of Justice regulating files containing data of a personal nature handled by the Property, Trade and Housing Registers and by the College of Property Registrars, Trade and Housing, the draft order updating the list of files containing data of a personal nature held by the Ministry of Development, the draft order for bringing into line the electronic files of the Ministry of the Interior and its public bodies containing data of a personal nature and creating new files that will be managed by the Ministry and public bodies, and the draft order extending and regulating the files containing data of a personal nature handled by the Ministry of Health and Consumer Affairs.

Norms of regional scope

The organic law on data protection laid down the competence of the autonomous communities' agencies, regulating in its Article 41.1 that the functions of their competence 'will be exercised when they affect files containing data of a personal nature created or managed by the autonomous communities or by the local administration or their territorial scope, by the corresponding bodies of each community, which will be considered as control authorities, and which will be guaranteed full independence and objectivity in the exercising of their functions'. In 2001, we had already reported that the autonomous community of Madrid approved a new data protection law that assigns competence to the Madrid Autonomous Community Agency in connection with the said files of the local administration and of the public right corporations that represent the economic and professional interests within the territorial scope of the said community. The following norms governing data protection affecting the scope of an autonomous community were approved in 2002 and 2003.

Catalonia

Law 5/2002 of 19 April 2002 creating the Catalonia Data Protection Agency.

Resolution GRI/2016/2003 of 1 July 2003 making public the Catalonia Regional Government Agreement of 23 June 2003 naming the director of the Catalonia Data Protection Agency and Resolution PRE/2094/2003 of 23 June 2003 naming the president of the Catalonia Data Protection Advisory Board.

Basque Country

Order of the head of the interior of the Basque Government regulating the electronic files containing data of a personal nature managed by the Department of the Interior and the autonomous body, Basque Country Police Academy, attached to it.

Madrid

Decree 67/2003 of 22 May 2003 approving the regulations developing the functions of the Madrid Autonomous Community Agency for data protection and the protection of rights and control over files containing data of a personal nature.

B. Changes made under the second and third pillars

The parliamentary processing of the law governing prevention and blocking of the financing of terrorism, on which we have already reported as starting in 2001, continued throughout 2002.

In 2003, two important new laws were adopted concerning the fight against terrorism, which complement each other and affect the field of data protection because they create new files in public ownership.

Law 12/2003 on preventing and freezing terrorism funding
This law sets up a Commission (Commission for Monitoring the Funding of Terrorist Activities) which has the authority to freeze funds, bank accounts and other financial assets belonging to entities or persons linked to terrorist activities. This Commission develops its competence within the administrative sphere but also collaborates with the judiciary and transmits its conclusions to the judge in criminal trials.

The law establishes the obligations of financial entities (banks, credit entities, exchange bureaus, etc.) and all subjects referred to in the law against money laundering (Law 19/2003, described below) to collaborate in providing all the information required (including personal data) in relation to frozen funds.

Where data protection in this respect is concerned, this law establishes that, for the effects of the national law on data protection (Law 15/1999), the files created by the Monitoring Commission will be considered files in public ownership (under the terms stipulated in Law 15/1999), which means that the exceptions regarding rights of access, rectification and cancellation (Article 23 of Law 15/1999) are fully applicable.

Law 19/2003, new regulation on the prevention of money laundering
Closely linked with the updated law, in July 2003 the law regulating the movement of money and international transactions was approved, which modifies the current law on the prevention of money laundering of 1993. The new rule incorporates into national legislation Directive 2001/97/EC on the prevention of money laundering.

The main aspects worth highlighting are as follows.

- Enlarged material scope: This law will apply not only to terrorist crimes, illegal drug trafficking and organised crime (current situation), but also to all other serious crimes (punishable with more than three years in prison) and related money laundering activities.

- Enlarged personal scope: The law imposes new obligations on subjects, such as auditors, external accountants (not only internal company accountants) and tax advisers. Notaries, lawyers and attorneys must also collaborate with full respect to professional secrecy and without prejudice to the constitutional right to defence.

- New obligations of information: The subjects listed above must demand to see clients' personal identification in the form of accredited documents, and to obtain information about their professional or economic activity; they are also obliged to reasonably check that such data are genuine.

  These subjects must also pay special attention to any complex or unusual operation conducted for no apparent lawful purpose; they must establish definite criteria for client admission, and they must communicate to a new body created by this law (the Executive Service for the Prevention of Asset Laundering under the authority of the National Bank of Spain) any transaction that fails to correspond with its declared nature, activity or background.

C. Major case-law

All the detailed statistical information on the appeals, judgments and specific analysis of each of the most relevant judicial findings are contained in the Data Protection Agency's 2002 and 2003 annual reports that are already available for consultation on its web page.

Here reference is made only to those judgments that have established precedents on the most controversial and hard to interpret aspects of the data protection law.

- Accuracy of the information contained in payment defaulter files: The judgment of 10 May 2002 dismissed the appeal and confirmed the criteria sustained by the Agency in the sense that the reflection of the piece of personal information 'balance 0' is not a true reflection of the real situation of the affected party, since the plaintiff had no balance whatsoever because the debt had been cancelled. The only reason that explains the continuance of the information in a file of personal wealth or solvency when the debt has been cancelled is to give information on the past defaults of the affected party, which is not congruent with the provisions of Article 4.3 of the data protection law, which requires that the current situation of the affected party be reflected, meaning the current solvency.

- 'Scoring' services: The national court has issued rulings on three occasions in connection with the provision, on the part of a certain services entity, of services of 'scoring' or evaluation of the financial situation of the clients of a third party that contracts the provision of such services. Thus, it is in order to cite the judgments of 18 January, 14 June and 15 November 2002, with the finding in all of these cases confirming the resolution issued by the Agency and, consequently, dismissing the appeal.

  The Tribunal's criteria (and that of the Spanish Data Protection Agency) is to consider that this practice constitutes a cession that has not been consented to by the affected party, because there is no record of any proof whatsoever accrediting the existence of a written contract between the entity requesting the information and the entity that provided the 'scoring' services and because the consent of the affected party for the preparation of the evaluation was not obtained. For the said practice to be considered within the scope of Article 12 of the data protection law, it is necessary for the way in which and the reason for which the data may be revealed to appear in writing in the contract concluded between the entity that requests the 'scoring' service and the entity that provides it.

- Data security: On 13 June 2002, the Contentious-Administrative Chamber of the National Court of Madrid dismissed an appeal against an Agency resolution of 21 May 2001 that sanctioned a particular entity for breaching the obligation to implement security measures as required by the data protection law and the regulations on security measures, based on the fact that documents that contained data of a personal nature for the internal use of the entity in question had appeared in refuse containers. The judgment confirmed the Agency's criteria that considered these facts as contrary to both Article 9 of the data protection law (security obligation) and Article 10 (obligation to secrecy).

  In addition, this event reached public attention because it was reported in various media.

- Cession of data: The judgment of 24 January 2003 establishes that there is cession of data when data are communicated by means of the Internet, clearly stipulating that images are data of a personal nature and that data handling exists when such images are emitted on the Internet. The judgment of 27 February 2003 establishes that it is the liability of the person ceding the data to obtain consent, and due diligence can be demanded of him/her.

- Payment defaulter files: The judgment of 9 May 2003 concerns notification of the inclusion in a payment defaulter file and examines the conditions required for such

inclusion to proceed. The judgment of 31 January 2003 studies the 'balance 0' status from the perspective of the organic law on data protection. The judgment of 14 February 2003 refers to personal property solvency, and studies negligence derived from the lack of internal communication on the settlement of a debt.

- Proceedings prior to a complaint: The judgment of 24 January 2003 stipulates the need to conduct initial proceedings regarding an event that gives rise to a complaint, and the problems derived from notifying a complaint to a specific address. The judgment of 21 February 2003 establishes that the complaint does not have to be communicated to the imputed party during the said prior proceedings, without this affecting the imputed party's right to a defence.

- Security measures: The judgment of 7 February 2003 refers to the security measures that must be adopted in relation to personal data processing. It also studies the presumption of innocence and onus of proof.

- Party liable for the handling of the protected legal property: The judgment of 28 February 2003 analyses the figure of the party responsible for the file in the public administrations sphere. The judgment of 28 March 2003 establishes that the protected legal property in the case of a complaint is privacy, without the need for a concurrent financial benefit to concur.

D. Specific issues

Parliamentary debates

Within the framework of institutional relationships that characterises part of the Data Protection Agency's activity, the Agency's Director appeared before the Congress of Deputies Constitutional Commission on 5 February 2003, with the purpose of reporting on the content of the 2001 annual report and replying to the questions raised.

During this appearance, the Director reported in detail on the development of the Agency's activity in 2001, with main reference to the register of files, citizens' advice, inspection, international relations, functions of adviser, and management of the required means for the Agency to operate correctly. Likewise, he replied to the questions raised by the parliamentary groups, especially in relation to security measures for the protection of personal data held by medical clinics, and the guarantee of the right to data protection of files used in staff recruitment processes.

Inspections

One of the fundamental activities of the Data Protection Agency is sectoral inspection programmes, which annually audit various sectors of both public and private standing, giving rise to the issue of the corresponding recommendations that must be fulfilled in a mandatory fashion, so as to bring into line the treatment given by the said sectors to the requirements laid down in data protection legislation.

During 2002, the sectoral inspections affecting the remote banking sector and the Register of Defaulters on Bills of Exchange (RAI) were completed; the body responsible for these activities is the Interbanking Cooperation Centre.

Some of the conclusions of the scheduled inspection of the remote banking sector were already presented in advance in the Data Protection Agency's annual report corresponding to the previous year. As a result of the said plan and within the year 2002, a final conclusions and recommendations document on the sector was drawn up, the entire text of which is reproduced in the Agency's 2002 annual report.

In turn, as a result of the investigations undertaken by the inspectors, certain deficiencies were observed in the information systems affecting the RAI files in connection with compliance with the provisions of Law 15/1999. For this reason, the corresponding recommendations were issued in 2002, which likewise are contained in the Agency's 2002 annual report.

In addition, throughout 2002, the Agency continued to promote the performance of sectoral inspections in a routine and scheduled fashion. The inspections carried out cover the treatment of personal data in competitions, games and draws on television, as well as the 2001 census project on population and housing undertaken by the National Institute of Statistics.

The conclusions and recommendations of all these inspections can be consulted in the Data Protection Agency's 2002 annual report.

In 2003, the sectoral inspections affecting hotel chains and competitions, games and draws on television aimed at finding the level of awareness and compliance of these sectors with regulations affecting data protection ended.

In addition, during 2003, the programmed inspections of education centres, laboratories and hospitals and Internet employment portals were initiated and the resulting recommendations and conclusions are scheduled to be issued in 2004.

Codes of conduct

Typified code of the Catalonia Hospitals Association (UCH)
The UCH code has been developed with the objective of defining a security policy in the treatment of personal health data, given their nature of specially protected information, and in the awareness of the appropriateness of establishing rules of conduct among its associates that allow the specific application of the legislation governing data protection, as a guarantee for the persons affected by the treatment of their data. For this reason, the code contains the criteria and conditions that must allow the construction of a body of good practice among the associates, aimed directly at guaranteeing, in the field of treatment of data relating to the health of the affected persons, standards of reference in strict compliance with the law.

Given the scope of specialisation that differentiates the organisations subscribing to the code, it has been created to become an efficient and rapid reference document for the medical sector, and social and social/health sectors concerning data of a personal nature, particularly those related to the individual's health, handled in files, such as generically denominated patient files or clinical histories.

Its main objective is to ensure that the subscribers to the code safeguard the privacy of the individual and guarantee the patient's rights where medical information is concerned.

Typified code on electronic commerce and interactive advertising
The companies that have promoted and subscribed to this typified code work in the field of commercial communications and the new electronic means of long-distance communication. The objective of its development is to provide a solution to the regulation problems in this sector, which, given its dynamic and permanently evolving nature, entails the possibility of regulations becoming outdated much more than in any other field, allowing it to adapt to change.

Likewise, it attempts to resolve the questions raised regarding the problems associated with the application of the existing legal regulations in the face of the unpredictable phenomena generated by the ever-more extended use of what are known as 'new technologies', and particularly the Internet.

Telefónica de España code of conduct
The typified data protection code of Telefónica de España, SAU, harmonises the values and principles that must guide the conduct of Telefónica de España in data protection matters with current developments in legislation affecting the telecommunications sector.

The code lays down the principles to which Telefónica de España actions will be subjected in the field of data protection, regulating the technical and organisational conditions for the existing current files, or new files that may be created in the future; likewise, it regulates the conditions for gathering and use of data, determining the procedure to be followed in exercising the rights of access, rectification, cancellation and opposition on the part of the affected parties as well as the specific rights of the consumers in the telecommunications sector.

In addition, Telefónica de España expresses its intention to extend this typified code to all the companies belonging to the Telefónica group. The typified code is applicable to all processing of data of a personal nature made in Spain by Telefónica de España, and serves as a point of reference in the different countries where companies belonging to the group are established, along with the desirable parameters that must be observed even when such data protection legislation is non-existent in the countries where those companies are located.

Activities of the Spanish Data Protection Agency concerning data protection in Iberoamerica
In the context of Iberoamerica, efforts are also being directed at achieving mutual cooperation and promoting personal data protection. The Spanish Data Protection Agency promotes the Iberoamerican Data Protection Conference on an annual basis. In 2003, this conference was held in La Antigua (Guatemala).

The concerns of the Iberoamerican countries that attended this conference have been reflected in its final declaration, which reiterates that personal data protection is a person's genuine fundamental right and recognises that the treatment of personal data can encourage the development of Iberoamerican countries within the framework of the information society. At the same time, it states the need to encourage the implementation of measures to guarantee a high level of data protection, and the ideal of having national regulatory frameworks, as well as highlights the importance of establishing a permanent channel of dialogue and collaboration in data protection matters. With this aim in view, the Iberoamerican data protection network was formed.

The countries that form this network undertake to collaborate on a mutual and permanent basis, with the objective of achieving harmonised solutions, and supporting initiatives to spread and develop data protection culture to Iberoamerican countries in a democratic context.

Agreements for collaboration with universities and public and private institutions
In 2003, the Agency also reached agreements with some institutions such as the Spanish University Conference of Deans and the Spanish Union of Tax Advisers, expressed through corresponding collaboration protocols, that establish a framework of joint activities that facilitate fulfilment of obligations in data protection matters. Likewise, this has stimulated the agreements for joint action signed in previous years with the High Council of the Chambers of Commerce, Industry and Navigation, the Professional Trade Union, the College of Property Registrars and General Board of Notaries.

E. Website

In this respect, one of the Agency's objectives fulfilled in 2003 has been the creation of a new web page and updating of the Agency's image with a new logo. These measures have been

aimed at offering the public greater ease of access and awareness of data protection matters, their rights and how to approach the Agency to defend them.

The new page (www.agpd.es) offers a wide range of information on data protection, including legislation and related documents of both national and international interest, the jurisprudence of the Spanish courts, typified codes inscribed in the General Data Protection Register, and the last annual report of the Agency's activities. The page also includes Agency reports that can be of great use for clarifying certain criteria for applying data protection regulations. In the near future, in fulfilment of Article 37 of the Spanish data protection law, modified by Law 62/2003 of 30 December 2003 on tax, administrative and social measures, 'the Spanish Data Protection Agency's resolutions will be made public once they have been notified to the interested parties', and taking into account that the law envisages that 'publication will be made preferably by electronic means', the said resolutions will be included on the web page.

Sweden

A. Legislative measures adopted under the first pillar

Although the Personal Data Act in principle applies generally to personal data processing in all sectors, there is specific regulation regarding certain sectors. A few examples of such specific regulation that was adopted in 2002 and 2003 are given below. As regards processing of personal data that falls under the scope of Directive 95/46/EC, the specific regulation must still be in accordance with the directive's provisions.

In 2002, a new Act of Parliament on Processing of Personal Data in Activity involving Employment Measures came into force. Another act of Parliament that came into force was the Act on Biobanks within medical care etc. Furthermore, the government adopted several ordinances regarding personal data processing, for example regarding processing of personal data in electoral activity and processing of personal data within the Swedish National Library's (Royal Library) project regarding long-term preservation of electronic documents (*Kulturarw*).

In 2003, a new Act on Processing of Personal Data within the Administration of Social Insurance came into force. Furthermore, Parliament adopted a new Act on Ethical Examination of Research with regard to human beings. This act came into force on 1 January 2004 and states that research which involves processing of sensitive personal data and personal data about criminal convictions without consent may only be carried out if it has been approved after an ethical examination.

B. Changes made under the second and third pillars

In 2002, no changes were made.

In 2003, Parliament adopted an ordinance on processing of personal data by the Swedish Coastguard in its criminal investigation activity etc. The ordinance requires that certain processing of data in this activity should be notified to the Data Inspection Board in advance for prior checking.

C. Major case-law

In 2002, the Supreme Administrative Court decided in a case regarding disclosure of personal data for direct marketing. In this case, a company asked the National Board of Student Aid for names and addresses of students for the purpose of sending them discount cards. The Data Inspection Board and later the Administrative Court of Appeal both made a balancing of

interest according to Section 10(f) of the Personal Data Act and found that the students' interest of privacy outweighed the company's commercial interest. The Administrative Court of Appeal stated that although many of the registered students would benefit from the company's offer, the students' interest of privacy still outweighed the company's commercial interest and, consequently, the company's use of the personal data would be in breach of Section 10 of the Personal Data Act. The company appealed to the Supreme Administrative Court which found that the National Board of Student Aid should disclose its file of students at universities for commercial purposes (direct marketing). The Court stated that the direct marketing literature was limited to being sent out once every half year, the personal data only included names and addresses and therefore could not be considered sensitive, and registered persons could oppose the direct marketing according to Section 11 of the Personal Data Act.

In the sixth annual report, the Data Inspection Board reported on a case regarding credit information on the Internet. The case had been brought to the Supreme Administrative Court and in May 2003 the Court gave its decision. The court case concerned a credit rating agency that had opened a website on the Internet, accessible only to subscribers to this service, where it published information about records of non-payment of debts regarding both natural and legal persons for the last three years. The agency claimed that the fundamental law on freedom of expression was applicable to the website. The Data Inspection Board found that the presentation on the website could not fall under the fundamental law and that the agency had to stop the publishing on its website. The agency appealed the Board's decision and the County Administrative Court as well as the Administrative Court of Appeal (both in Stockholm) found that the fundamental law on freedom of expression would apply. The Data Inspection Board then brought the case to the Supreme Administrative Court which upheld the lower courts' decisions and thus rejected the Data Inspection Board's appeal.

D. Specific issues

In 2002, the government assigned a commission of inquiry to review the Personal Data Act with the task of — within the framework of the EC directive —determining the possibilities of bringing about a regulation that aims more at the prevention of abuse of personal data than the regulation of all steps of the processing of such data (the commission submitted its report in January 2004).

With reference to the outcome of the abovementioned court case regarding credit information, it could also be mentioned that the Ministry of Justice has started an investigation regarding the rules of the Credit Information Act in relation to the rules of the fundamental law on freedom of expression as to publishing on the Internet. The results of the investigation will be presented on 1 August 2004.

In November 2003, the Court of Justice of the European Communities delivered its preliminary ruling in Case C-101/01 *Lindqvist* v *Office of the Public Prosecutor in Jönköping* concerning publishing of personal data on a website. The Göta hovrätt (Court of Appeal) had in the criminal proceedings requested the Court of Justice to give a preliminary ruling regarding the interpretation of certain aspects of Directive 95/46/EC. The Göta hovrätt has not yet (March 2004) decided on the case.

In 2003, the Data Inspection Board published guidelines regarding the interpretation of the Personal Data Act. The following guidelines were published: 'Retention of personal data', 'Balancing of interest according to the Personal Data Act' and 'Consent according to the Personal Data Act'.

E. Website

www.datainspektionen.se

The website is available in English and Swedish.

United Kingdom

A. Legislative measures adopted under the first pillar

See 'Specific issues' below.

B. Legislative measures adopted under the second and third pillars

See 'Specific issues' below.

C. Major case-law

The years 2002 and 2003 saw a number of cases heard which have been important in developing jurisprudence in the area of privacy law. Many of these cases have been high profile and have involved the consideration of two competing human rights, the right to private and family life and the right to freedom of expression, typically in the context of newspaper reports about the private lives of celebrities.

There have also been significant judgments which have looked at the very nature of personal data and which have had considerable implications for the application of the Data Protection Act 1998 especially the right of access. These have cast considerable doubt upon the use of subject access as a means of obtaining disclosure of documentation/information outside the normal rules provided by the courts for such issues in the context of legal claims/proceedings.

The Information Commissioner v *Islington Borough Council:* The case established an important principle, that the knowledge and actions of directing minds of a corporate body must be taken together with the actions of those to whom administrative functions are delegated in determining criminal responsibility for the actions of the corporate body.

P. v *David Wozencroft:* The case established that the right to go to court under the Data Protection Act 1998 does not exist in isolation and will be considered subject to the procedural rules of the courts. The case suggests that the courts are less likely to entertain cases brought under the Data Protection Act 1998 challenging the accuracy of information where an opportunity to challenge the same personal information has been afforded the individual in an earlier separate claim.

Naomi Campbell v *MGN Limited:* The case was heard by the Court of Appeal and confirmed and clarified various routine matters of interpretation for Directive 95/46/EC and the Data Protection Act 1998. The Court confirmed that the definition of processing under the act is very wide and that publication will be treated as part of the operations covered by the act. The judgment was appealed to the House of Lords with a judgment expected in 2004.

Durant v *Financial Services Authority:* This case saw the learned judge applying a highly restrictive interpretation of the definition of a relevant filing system. The judgment was appealed with the Court of Appeal upholding the judge's ruling at the end of 2003. The ruling has also had a considerable role in clarifying the definition of personal data, linking it to information which affects an individual's privacy.

Re Terrence Patrick Ewing: A High Court judge ruled that an appeal to the Information Tribunal under Section 28 of the Data Protection Act 1998 constitutes civil proceedings and that the Information Tribunal is a court for the purposes of the act.

R (On behalf of Alan Lord) v *The Secretary of State for the Home Department:* The Court confirmed and clarified various routine matters of interpretation of the Data Protection Act 1998. It considered the limitations on the right of access provided by Section 29 (the exemption for crime prevention and detection), Section 7(4) to 7(6), Section 8(2)(a) and Section 7(9) of the Data Protection Act 1998. The learned judge agreed with the Data Protection Tribunal's analysis in *Equifax Europe Ltd* v *The Data Protection Registrar* (Case DA/90 25/49/7) that the words 'in any case' in Section 29(1) of the Data Protection Act 1998 are to be read as meaning 'in any particular case'. The judge also agreed with the Data Protection Tribunal's analysis of the word 'likely' in the context of Section 29.

For further information about these cases and others which covered the Data Protection Act 1998 and Directive 95/46/EC, see the Information Commissioner's annual report for the years ending March 2003 and March 2004, available at http://www.informationcommissioner.gov.uk/eventual.aspx?id=279.

D. Specific issues

In 2002, there were two statutory instruments made under the Data Protection Act 1998. These were the Information Tribunal (Enforcement Appeals) (Amendment) Rules 2002 and the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002.

The year 2002 saw the UK Government hold a consultation on a proposal for introducing 'entitlement cards'. It was pleasing to note that the government fully recognised that this important issue raised substantial data protection and privacy concerns that have to be addressed if any scheme was to proceed. We commissioned academic research and held a conference which fed into the very detailed consultation response that we provided. We acknowledged that data protection legislation did not prohibit such a scheme but that the proposals would have to be significantly developed to demonstrate compliance with the requirements of the Data Protection Act 1998 and Human Rights Act 1998.

In 2003, the Home Office published a document entitled 'The next steps', which sets out the government proposals for a draft bill on entitlement/identity cards. We have had continued dialogue with the Home Office about the proposals. The Parliamentary Home Affairs Select Committee began an inquiry into the proposals at the end of 2003 which we will give evidence to in 2004. We continue to hold the view that the proposals need to be significantly developed to demonstrate compliance with requirements of the Data Protection Act 1998 and that the necessary safeguards must be in place from the outset of any such scheme.

During 2002, the Lord Chancellor's Department conducted a review of the rights of access under the Data Protection Act 1998. We welcomed this review as the interface between these rights and the rights of access under the Freedom of Information Act 2000 is of particular importance to us. No action has yet been taken as a result of this review.

The Anti-Terrorism and Security Act 2001 included provisions for communications providers to retain communications data for national security purposes. The data would therefore be retained for longer than is necessary for the service providers' own business purposes. During the passage of the act, we expressed concerns that the retention may not be a proportionate response to the perceived problem and we continue to have those concerns. In 2002, we

assisted the Home Office in developing a code of practice under which service providers can reconcile longer retention periods and the requirements of the Data Protection Act 1998.

We also responded to a number of governmental consultations during 2002. In our response to a consultation following a review of the Rehabilitation of Offenders Act, we welcomed the suggestion for a code of practice on employers' use of information about individuals' criminal convictions and for a shortening of the rehabilitation period.

In a response to a Treasury consultation on proposed amendments to the money laundering regulations of 2001, we commented on the proposal that additional personal data should be included with all wire transfers of money in order to implement a Financial Action Task Force special recommendation concerning terrorist financing. We expressed the view that an order should be made under Schedule 4, paragraph 4(2), of the Data Protection Act 1998 to place beyond doubt that transfers of these transfers of additional personal data outside the European Economic Area were necessary for reasons of substantial public interest.

In 2003, we commented on a number of codes of practice produced by other organisations and the government including proposals for national archives legislation, the electronic communications regulations, the further use of electoral registers, voluntary retention of communications data, and the use of personal data in extradition proceedings.

We also continued to respond to a number of government proposals in 2003: a bill on gender recognition; proposals for local authorities to hold information on every child in the UK and information about those who care for them; a register of county court judgments; information powers in connection with asylum and immigration; and information processed during children's hearings.

During 2002 and 2003, we continued to work on our Employment Practices Data Protection Code. We are producing the code to clarify what data protection law requires and to help employers negotiate this difficult area of the law. We have so far produced three of the four parts of the code and we are reaching the end of the consultation period for the fourth part.

E. Website

www.informationcommissioner.gov.uk

1.5. European Union and Community activities

1.5.1. Nomination of the European Data Protection Supervisor

Following the provisions of Article 286 of the EC Treaty, Regulation (EC) No 45/2001 of the European Parliament and of the Council 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 ([6]) applies the Community rules on data protection to the processing of personal data carried out by the Community's institutions and bodies. It provides, *inter alia*, for the establishment of an independent supervisory authority called the 'European Data Protection Supervisor (EDPS)' and for an 'Assistant Supervisor'.

Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the

([6]) OJ L 8, 12.1.2001, p. 1.

performance of the European Data Protection Supervisor's duties ([7]) determined that the authority's seat be in Brussels, and that the position of the European Data Protection Supervisor be put on the same footing as a judge of the Court and that the Assistant Supervisor be put on the same footing as the registrar of the Court of Justice.

In accordance with Article 42 of the regulation, the European Parliament and the Council appoint by common accord the European Data Protection Supervisor and the Assistant Supervisor for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates. The Commission launched the open call for candidates on 20 September 2002 and submitted a list of nine candidates to the European Parliament and the Council for both positions on 23 April 2002. As a result of these procedures, the European Parliament and the Council nominated Mr Hustinx as Supervisor and Mr Bayo Delgado as Assistant Supervisor on 22 December 2003 ([8]).

1.5.2. Judgments of the Court of Justice

The Court of Justice ruled twice on the interpretation 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 (OJ L 281, 23.11.1995, p. 31) in 2003.

Interestingly, the Court held in both cases that as far as the scope of the directive is concerned that it does 'not presuppose the existence of an actual link with free movement between Member States in every situation'. Therefore, the directive is applicable to situations that do not involve movement of data between several Member States, only unless the explicit exceptions apply (such as public security, defence, or purely personal activities), which the Court interprets restrictively.

A. JOINED CASES C-465/00, C-138/01 AND C-139/01 *RECHNUNGSHOF*, JUDGMENT OF THE COURT OF JUSTICE OF 20 MAY 2003

Rechnungshof (C-465/00) v *Österreichischer Rundfunk and Others* and *Christa Neukomm* (C-138/01) *and Joseph Lauermann* (C-139/01) v *Österreichischer Rundfunk*

References for a preliminary ruling: Verfassungsgerichtshof (C-465/00) and Oberster Gerichtshof (C-138/01 and C-139/01) — Austria.

European Court reports 2003, I-4989

Questions were raised in proceedings between, first, the Rechnungshof (Court of Audit) and a large number of bodies subject to its control and, second, Ms Neukomm and Mr Lauermann and their employer Österreichischer Rundfunk (ORF), a broadcasting organisation governed by public law, concerning the obligation of public bodies subject to control by the Rechnungshof to communicate to it the salaries and pensions exceeding a certain level paid by them to their employees and pensioners together with the names of the recipients, for the purpose of drawing up an annual report to be transmitted to the *Nationalrat*, the *Bundesrat* and the *Landtage* (the Lower and Upper Chambers of the Federal Parliament and the provincial assemblies) and made available to the general public.

([7]) OJ L 183, 12.7.2002, p. 1.

([8]) Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty (European Data Protection Supervisor) (OJ L 12, 17.1.2004, p. 47).

The Court held:

1. Articles 6(1)(c) and 7(c) and (e) 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 do not preclude national legislation such as that at issue in the main proceedings, provided that it is shown that the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Rechnungshof but also of the names of the recipients of that income is necessary for and appropriate to the objective of proper management of public funds pursued by the legislature, that being for the national courts to ascertain.

2. Articles 6(1)(c) and 7(c) and (e) of Directive 95/46 are directly applicable, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions.

B. CASE C-101/01 *LINDQVIST*, JUDGMENT OF THE COURT OF JUSTICE OF 6 NOVEMBER 2003

Criminal proceedings against Bodil Lindqvist.

Reference for a preliminary ruling: Göta hovrätt — Sweden.

European Court reports 2003 (not yet published): OJ C 7 (2004), p. 3

Questions were raised in criminal proceedings against Mrs Lindqvist who was charged with breach of the Swedish legislation on the protection of personal data for publishing on her Internet site personal data on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church.

The Court held:

1. The act of referring, on an Internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) 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.

2. Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.

3. Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.

4. There is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an Internet page which is stored on an Internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the Internet, including people in a third country.

5. The provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined *inter alia* in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.

6. Measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.

1.5.3. First Commission report on the implementation of the directive in the European Union

Article 33 of the data protection directive foresees that the Commission shall review the implementation of the directive three years after the period of its adoption, that is in October 2001. Given that most Member States were late in its transposition, the Commission decided to delay this report by some months and it organised in the meantime an information gathering exercise by which Member States, data protection authorities and representatives of data controllers would be given the opportunity to express their views on the implementation of the directive in the Member States.

The 'review of the directive' concluded in November 2002 with an international conference hosted by the Commission in Brussels. At that occasion, most participants agreed that it would be too premature for the Commission to attach amendments to the directive but rather it would be necessary in any case to address some of the most serious shortcomings detected by operators. The first Commission report on the implementation of the data protection directive, adopted on 15 May 2003, loyally reflected the results of the debates and enclosed a work programme aimed at improving the implementation of the directive in the Member States. This was envisaged by a myriad of tools, the most prominent of which are dialogue with the Member States, infringement cases where necessary, 'soft-law' approaches with the participation of the Article 29 Working Party, and the promotion of privacy enhancing technologies.

The Article 29 Working Party, in particular, was called on to play a key role in the carrying-out of this work programme, a role that was acknowledged by the Working Party in its priorities for its work programme for 2003 and 2004.

As regards the appraisal of the data protection directive, the findings of the report were overall positive: the directive had fulfilled its principal objective of removing barriers to the free movement of personal data between the Member States while guaranteeing a high level of protection for the privacy of individuals. However, the report expressed concerns about excessive differences in the way that Member States apply and interpret national laws adopted pursuant to the directive. Data protection authorities in the Community may, in the views of the Commission, lack sufficient powers or resources to accomplish their monitoring tasks.

This important report was welcomed by most operators, the Member States and the European Parliament and set out the main lines of the European Commission's policy on data protection for the years to come. It was announced that the results of the work programme for better implementation of the directive would be presented and assessed by the Commission in 2005.

2. PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES

2.1. European Economic Area

Iceland

A. Legislative measures adopted under the first pillar

In the years 2002 and 2003, a number of acts and regulations under the first pillar concerning data protection were passed. These are the most important ones.

1. Act on Child Protection (No 80/2002): According to Article 36 of this act, superiors in schools, kindergartens, summer camps, sports and hobby centres, and other similar institutions and places where children gather have the right to obtain information from the Central Criminal Register on job applicants. However, the applicants must have given their consent to the obtention of this information.

   The provision on consent was, originally, not in the bill to the act. The Data Protection Authority (DPA) criticised that, and the bill was consequently changed so that consent from the individuals concerned should be acquired.

2. Act No 81/2002 on an amendment to the Act on the Protection and Processing of Personal Data (No 77/2000): This act clarifies the Data Protection Act's provisions on electronic surveillance and the information to be given to the data subject.

3. Act on Foreigners (No 96/2002): According to Article 54 of this act, the Minister for Justice can pass rules on the duty of hotels, hostels, camps, etc., to keep registers of guests and notify the police of them. The rules may also impose the duty on others, i.e. those who have foreign night-guests in their private homes, to notify the presence of these guests to the Directorate of Immigration if it is deemed requisite on the grounds of security reasons or specific preparation. The DPA criticised this provision when the bill to the act was in the Authority's hearing.

   The Minister for Justice has now passed a regulation based on the Act on Foreigners, i.e. the regulation on foreigners (No 53/2003). According to Article 107 of this regulation, hotels, hostels, camps, etc., must keep registers of their guests, i.e. forms that the guests fill in themselves. The police may access the registers at any time, and they must be retained for two years. However, the regulation does not impose the duty of registration and notification of foreigners on those who have foreign night-guests in their private homes.

   According to Article 55 of the Act on Foreigners, the processing of personal data, be it sensitive, is allowed to the extent it is necessary for the execution of the act. The police and the Directorate of Immigration's registers may be linked as occasion requires. Before passing rules on which registers on foreigners the police and the Directorate of Immigration may keep, the Minister for Justice must obtain the DPA's opinion.

4. Act No 46/2003 on an Amendment to the Act on the Protection and Processing of Personal Data (No 77/2000): This act clarifies the Data Protection Act's provisions on electronic surveillance.

5. Act on Telecommunications (No 81/2003): By Articles 42 to 48 of this act, the provisions in Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector were implemented (however, this directive is still not part of the EEA Agreement).

6. Act No 89/2003 on an Amendment to the Medicinal Products Act (No 93/1994), and the Act on Doctors (No 53/1988): By this act, the Medicinal Products Act was amended so as to provide for two central electronic databases containing information from pharmacies on all prescriptions (Articles 25 to 27 of the Medicinal Products Act). One of these databases shall be personally identifiable, but the identity markers shall be encoded. It shall be run by the Directorate of Health which shall use it in connection with its surveillance of doctors' prescriptions, i.e. whether they are giving too many prescriptions to certain individuals etc. The Medicinal Control Agency shall also have access to the database for its surveillance of whether prescriptions have been falsified or otherwise unlawfully made and whether they have been dispatched in a wrong way. Additionally, the State Social Security Institute shall have access to the database for its surveillance of medicine costs and also for reimbursing patients' costs of the use of medicine. In the first case, personal identifiers may not be used, and, in the latter case, the patients must have given their consent for the processing of their information.

   The other database shall be non-personally identifiable. When information has been retained for three years in the first database, it shall be erased from it and put into this non-personally identifiable database. It shall be run by the State Social Security Institute and used for statistical purposes.

7. Rules on the Treatment of Applications for Access to Clinical Records in Connection with Retrospective, Scientific Research (No 340/2003): According to the Act on the Rights of Patients (No 74/1997), the access to clinical records in scientific research must be authorised by the DPA. Often, the Authority's permissions stipulate that the patients must consent to their clinical records being accessed. In other cases, however, the Authority does not stipulate this since it would lay heavier burdens on the data processor than can be considered fair, for example when it is necessary to work with a very big research group so that the aim of the research project can be fulfilled. In these cases, Rules No 340/2003, passed by the DPA in accordance with Article 37 of the Data Protection Act, govern the treatment of applications for access to clinical records. Also, there are provisions concerning how data obtained for research purposes shall be protected once they have been accessed.

B. Changes made under the second and third pillars

The main change in legislation concerning other pillars than the first was the amendment of the Traffic Act (No 50/1987) by Act No 83/2002. The amendment provides for a new institution, the Road Traffic Directorate, which shall, according to Article 112 of the Traffic Act, have the task of running computer and information systems. In addition to the computer and information systems that concern traffic, for example the Car Register, the Road Traffic Directorate runs non-traffic-related computer and information systems. Of those, the most important is the Schengen information system in Iceland.

C. Major case-law

On 27 November 2003, the Supreme Court of Iceland delivered a judgment in a case concerning the planned Icelandic health sector database, which the company deCode/Íslensk erfðagreining is planning to build. According to law, health information from clinical records on all Icelanders will be put into this database without consent, but people have the right to abstain. A woman did not want information on her late father to be put into the database. She was denied this since the act concerning the database only grants this right to the data subject him/herself. However, the Supreme Court came to the conclusion that her claim should be accepted because health information on her father could be relevant in assessing her own health. Also, in the light of the Constitution of Iceland, which grants everyone the right to privacy, the Supreme Court considered the act concerning the database to be too vague in

terms of data security. This applied, for example, to encryption of data, which is supposed to make them unidentifiable. Likewise, this applied to security when matching the data in the health sector database with data in a genealogical database and a genetic database.

D. Specific issues

One of the main tasks that the DPA undertook in 2002 and 2003 was inspections. In the latter year, formal administrative decisions were taken regarding inspections that began in 2002 and also in 2001. The two big pharmacy chains in Iceland were, by decisions delivered on 3 July, required to satisfy a number of demands for higher security of personal data. Also, on 27 August, a decision regarding the security and legitimacy of personal data processed by the Medicinal Control Agency was delivered and the Agency was required to satisfy a number of demands in that respect. Additionally, on 4 December, a conclusion regarding the security of biosamples and other personal data processed by the biobank of the National University Hospital was delivered in which it was required that a number of demands be satisfied in that respect. It will be determined at a later time whether the demands, laid down in these decisions, have been met.

In addition to these decisions, the DPA delivered, on 2 September 2003, a formal opinion in connection with an inspection of the security of personal data in the planned electronic clinical records system for the East Iceland Health Institution, combining all the institution's electronic clinical records in one system, called Saga. The main result was that the security of personal data was high enough, but that, in some instances, more measures would, however, have to be taken.

E. Website

The Icelandic DPA, Persónuvernd, has the following website address: http://www.personuvernd.is. Under 'Information in English', a number of acts and other information, for example on the judgment of the Supreme Court of Iceland of 27 November 2003, can be found.

Liechtenstein

2002

The date 1 August 2002 saw the entry into force of the Data Protection Act (DSG, LGBl. (Liechtenstein Official Gazette) 2002, No 55) and its implementing Data Protection Ordinance (DSV, LGBl. 2002, No 102). This transposes Directive 95/46/EC. The creation of the DSG simultaneously amended the Act on Individual Contracts of Employment (LGBl. 2002, No 56) by introducing the stipulation that the employer may process employee data only if such data concern the individual's suitability for work or to implement a contract of employment. The DSG created an independent Data Protection Commissioner and Data Protection Commission (DSK). The Data Protection Commissioner may issue recommendations, whilst the DSK has competence to issue decisions in data protection matters. The government appointed Dr Philipp Mittelberger as Data Protection Commissioner. The President of the three-person Data Protection Commission, which was elected by the Parliament (*Landtag*) for a period of four years, is Dr Marie-Theres Frick.

2003

The main task of the Data Protection Commission in the first full year of its activity was to create a functioning infrastructure, raise public awareness about data protection and deal with basic data protection issues.

In addition to a number of newspaper interviews, an article on data protection was published in the June edition of the Liechtenstein Law Journal. Furthermore, the end of August saw the Data Protection Commission's website come online on the German language Liechtenstein Government portal (www.sds.llv.li). Unofficial translations of both the Data Protection Act and Data Protection Ordinance can be downloaded from this site. A number of events were also organised to raise awareness about data protection.

The DSG makes provision for various types of advisory functions on the part of the Data Protection Commissioner. These basically involve providing assistance for private individuals and the authorities in the form of general guidelines, and providing advice and opinions on bills and ordinances that are relevant to data protection. Advisory functions took pride of place during the reporting period. Of a total of 243 registered requests, 100 concerned the disclosure of data by the authorities. Much-needed guidelines were issued on data disclosure by the Liechtenstein authorities and by the municipalities in the course of checks on residents.

Opinions were issued on a number of draft laws. These included, in particular, opinions concerning pending work on legislation, some of which entered into force during the reporting year, namely those listed below.

- The Road Traffic Act was modified by LGBl. 2003, No 139, creating a register of vehicles and vehicle owners, a register of administrative measures and a driving entitlement register. The government was also granted authorisation to conclude agreements with Switzerland on participation in the management and use of automated Swiss registers akin to those described above, subject to data being protected.
- The Medical Practitioners Act (LGBl. 2003, No 239) creates a specific basis for a register of medical practitioners to be kept by the Chamber of Medical Practitioners.
- The Sickness Insurance Act (KVG) was supplemented by LGBl. 2003, No 241, which introduced a machine-readable sickness insurance card and ID number. This card may also include health data and personal profile if the insured party gives his/her consent.
- The Electronic Signatures Act (LGBl. 2003, No 215) establishes the legal framework for the creation and use of electronic signatures and for the provision of signature and certification services, particular attention being paid to the legal ramifications of electronic signatures and the rights and obligations of signatories and those providing certification services. It transposes Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ('signatures directive', EEA law: Annex XI — 5g.01).

Judicial decision: On 7 May 2003, the former Administrative Complaints Court (now the Administrative Court) issued a decision on Article 36 of the Banking Act (LGBl. 1992, No 108). This states that, in the course of international cooperation between the authorities, client data can and must be transferred abroad, providing the principles of speciality, confidentiality, 'long hand' (°) and proportionality are complied with. The provisions of the Data Protection Act, particularly Articles 2 and 8, are not in conflict with the provisions governing cooperation between the authorities as set out in Article 36 of the Banking Act. The decision can be downloaded from http://www.llv.li/pdf-llv-sds-vbi_entscheid.pdf.

Register: Setting up the public register of data collections was extremely time consuming, and it was not possible to complete the work during the reporting year. By 31 December 2003, 409 registrations had been summarily checked for accuracy. The plan is to publish the register on the Data Protection Commission's website. Preparatory work is under way.

(°) The Liechtenstein Supervisory Authority may forward publicly inaccessible information and documents to foreign supervisory authorities only if the said foreign supervisory authorities do not, without the prior consent of the Liechtenstein Supervisory Authority or by virtue of a general authorisation clause in an international treaty, forward such information to competent authorities and to other bodies which carry out supervisory functions in the public interest.

Norway

A. Significant changes to privacy or data protection law

The new Personal Data Act and regulations entered into force on 1 January 2001. The act implements Directive 95/46/EC and replaces older legislation on the subject. Transition arrangements from prior legislation ceased at the end of 2002.

The Personal Health Data Filing Systems Act on the processing of personal health data entered into force on 1 January 2002, and applies to the processing of personal health data for public health administration and public health services that takes place wholly or partly by automatic means. The act is based on the same principles as the Personal Data Act.

The two abovementioned acts became valid in their entirety on 1 January 2003.

B. Significant changes to other laws affecting privacy or data protection

The Immigration Act: Fingerprint register for foreigners
When immigration authorities in 1992 decided that they could request that foreigners provide fingerprints, the clear goal was that they would be used as an aid for identifying the person in connection with their applications for asylum and residency. Already at that time, the Data Inspectorate expressed concerns that there would be pressure for use of the fingerprint register for other purposes. The Data Inspectorate is critical of a register being created for one purpose (identification) that could also be used for other purposes (investigation of crimes). Thus, the Data Inspectorate set a requirement in the licence for the register that a warrant must be issued before the police can use the data in their investigation duties.

This legal protection guarantee has now been revoked, and the police have been given legalised access to search the immigration authorities' fingerprint registry.

Terrorism stipulations in the Criminal Act and storage of traffic data
The Criminal Act and Criminal Procedure Act have their own stipulations on terrorism. Planning and preparation of terrorist actions have been made punishable through an amendment to the Criminal Act. The amendment consists of legal provisions regulating a possible sentence of up to 12 years' imprisonment for planning and preparing terrorist actions. Two partially overlapping working groups are now evaluating the need for easier access for the police to use extraordinary methods of investigation, such as technical tracking and different forms of communication control, as means against crime and terrorism. A third working group looks into questions regarding cybercrime prevention. In anticipation of this group's report, the Parliament has provided the legal basis to require traffic data from telecommunication systems to be retained for a hitherto undefined period after the original purpose is fulfilled. This possibility has not yet been used.

Money laundering — widened duty to report
A new law on preventive measures against laundering of capital gains and financing of terrorism has been implemented. Both the group of those who are required to report and what kinds of situation that shall be reported are widened. Even lawyers have had the duty imposed to report in certain settings.

New law on biobanks
A new law on biobanks has been implemented. The law regulates the collection, storage, processing and destruction of human biological material and data as a result of these. The provisions on explicit, voluntary and informed consent from the giver of the material is central to the law.

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

Guideline for collection of personal data
Both the Personal Data Act and the Marketing Control Act set limits for what kind of personal data companies that do business over the Internet can collect and use. However, many companies are unsure about the interpretation of the legislation and rules, and how the requirements are to be fulfilled in practice. This is the reason the Consumer Ombudsman (who conducts inspections according to the Marketing Control Act) and the Data Inspectorate have together created a guideline on collection and use of personal data on the Internet for companies to use. The guideline is adapted to sale and purchase of goods on the Internet conducted by adult users.

Guideline for the use of consent from minors
A separate guideline is provided for the use of consent from under-aged children. The guideline states at which age the youngster him/herself can consent to the processing of his/her own personal data.

Data protection officials
Since 2001, the Data Inspectorate has worked towards setting up a voluntary arrangement for the establishment of data protection officials in companies that process personal data. As a result of this work, the first data protection officials were established. Many organisations have thus been exempt from notification duties (notifying of processing of personal data to the Data Inspectorate), referring to their use of data protection officials. Before organisations can be exempted from notification duties, the data protection officials must participate in an obligatory seminar, where they receive a basic introduction to the regulations and the tasks they take on as data protection officials.

D. Website

The Data Inspectorate's website is at http://www.datatilsynet.no.

2.2. Candidate countries

For all the candidate countries, the reinforced pre-accession strategy aims at allowing their integration of the Community *acquis*. In this spirit, the European Commission monitors both the adoption of legislation transposing EU law, in particular Directive 95/46/EC, and the establishment of the administrative structures necessary for its effective implementation, such as independent data protection supervisory authorities.

Developments in this field took place in a number of candidate countries. New data protection legislation was adopted in 2002 in Latvia and Slovakia, and in 2003 in Estonia, Hungary and Lithuania. In 2002, peer reviews by experts from data protection authorities of EU Member States took place in the Czech Republic, Hungary and Poland.

Cyprus

In November 2001, the processing of personal data (protection of individuals) law of 2001 came into force in Cyprus. The law implements Directive 95/46/EC. It provides for the appointment of a Personal Data Protection Commissioner, who is an independent officer of the Republic, and who has the responsibility of supervising the application of the law. The law also provides for the establishment of the Office of the Commissioner. The Commissioner, Ms Goulla Frangou, was appointed for a term of four years commencing on 1 March 2002, and the Office of the Commissioner was established in May 2002.

After the establishment of the Office of the Commissioner, the procedure for the submission of notifications has been put in place and regulations were issued which prescribed the fees to be paid for the licences for the transmission of data and the combination of files.

During the period from May 2002 to December 2003, 1 370 notifications were submitted.

During the same period, a number of seminars were organised, as well as speeches to professional bodies (banks, insurance companies, municipalities) mainly focusing on raising awareness between the data controllers.

During the period under review, the Office of the Commissioner received a small number of complaints. It is worth mentioning that all the complaints were resolved by reaching an agreement with the data controllers.

A number of licences for the transfer of personal data to third countries were granted.

A twinning light project for enhancing the capacity of Cyprus to apply the data protection principles took place during 2003 with experts from the United Kingdom.

A workshop was organised with the cooperation of the Council of Europe in order to train government officials on their responsibilities as data controllers.

Looking ahead, the Office of the Commissioner plans to continue its awareness campaign both amongst the citizens, in general, and controllers, in particular. To this end, guidance for specific issues of data processing is going to be issued.

The website of the Commissioner's Office (www.dataprotection.gov.cy) was created in 2003.

Czech Republic

On 4 April 2000, the new Personal Data Protection Act (Act No 101/2000 Coll., on the Protection of Personal Data and on Amendment to some Related Acts, as amended later) was enacted and entered into force on 1 June 2000. The act replaces the Act on Protection of Personal Data in Information Systems 1992. The new act almost entirely implements the requirements of the EU data protection directive. In accordance with the directive, it grants exceptions from several key provisions in the field of public and national security to the police, intelligence services and some other bodies. The European Commission in its 2002 regular report on the Czech Republic's progress towards accession stated: 'Legislation in the field of the protection of personal data is largely in line with the *acquis*. However, amendments to the 2000 [Personal] Data Protection Act are still needed to make it fully compliant with the *acquis*.' At the end of 2003, the Czech Government approved a draft amendment to the Personal Data Protection Act which, after having passed through Parliament, will ensure full alignment with the EU *acquis* in the last remaining details. The amended act is supposed to enter into force on 1 May 2004.

On 1 June 2000, an independent supervisory authority — the Office for Personal Data Protection (OPDP) — was established by the abovementioned Act No 101/2000. The Office is endowed with all standard powers and is successively developing all standard activities and functions of an independent national EU data protection supervisor — such as data processing registration, control, taking measures including direct sanctions, issuing permissions for transborder data flows, consulting, and data protection awareness enhancement. The independence of the OPDP is guaranteed by the act and by the way of appointment of its President and of seven independent inspectors, who are named by the President of the Czech Republic on a proposal from Parliament (Senate) for a period of five years (the President of the Office) and 10 years (the inspectors). The OPDP has its own chapter in the State budget. The Office also had authority over the accreditation and control of the certificate authorities for digital signatures under Act No 227 of 29 June 2000 on Electronic Signatures but since 1 January 2003 this competence has been transferred to the new Ministry of Informatics.

The year 2002 was a very important year for personal data protection in the Czech Republic. Under the influence of global events, the aspect of personal data protection became so widely recognised that there was no need to persuade the public as to why personal data should be protected, but rather it was necessary to explain how such data can be protected. The Czech Republic declared that respect for human rights is amongst its permanent priorities. After ratifying Council of Europe Convention No 108 in 2001, in April 2002 it also signed the additional protocol to this convention and initiated the legislative process for its ratification.

The international evaluation of the quality of personal data protection in the Czech Republic culminated in the evaluation mission of the European Commission — the peer review, which assessed the work of the Office. The team of EU experts came to the following conclusions: 'The peer review team was impressed by the achievements made by the Czech Data Protection Authority in such a short period of time since its establishment in 2000. It is a very well known, regarded and respected authority which fulfils in practice every aspect and condition present in Article 28 of Directive 95/46/EC. All the departments conduct their activities with high concern and on a high level of knowledge. At this point, it is worthy to mention that almost all the departments are understaffed. This happens mainly for two reasons. The first one is the lack of physical room in the current premises of the UOOU to accommodate more staff complying with the labour regulations on this respect. For that reason, the peer review team would like to make a point on the necessity of the UOOU of being provided with adequate premises not to jeopardise its full operation. Secondly, there is also a structural problem relating to the difficulty of hiring qualified staff (mainly law experts) due to the huge difference between the salaries these professionals earn in the private sector

and the ones the Office can offer which are established according to the public employees rules. Besides, due to the important international activity of the Office and its very active participation in the different international fora already mentioned in the report, it would be advisable, through the available programmes, the Office could apply to the European Union institutions to obtain some additional funding for more people could be involved in missions abroad which could help to increase the expertise of its staff in these matters.'

As of December 2002, a total of 20 143 data processings notified by 17 703 controllers had been registered with the Office, of which in 2002 the Office registered 3 061 data processings notified by 3 967 controllers. In 2002, the Control Department of the Office dealt with 755 complaints and petitions; the most frequent complaints that the Office found to be justified concerned the following shortcomings in personal data processing: (i) unclear sources of data used for addressing potential clients in direct marketing; (ii) extensive use of birth certificate numbers; (iii) systematic acquisition of video recordings of individuals; (iv) list of debtors publishing; (v) insufficiencies in the formulation of the data subject's consent and in the conditions under which it is provided, etc. Justified complaints together with the plan of controls led to 354 investigations (inspections and other control actions). The main sectors to which the investigations were related were public administration (80 actions), banking (49 actions), marketing (32 actions), trade (31 actions), health and social services (26 actions), etc.

The provision of Article 27 of the Personal Data Protection Act imposes on the Office the obligation to hold administrative proceedings connected with issuing decisions on permitting or rejecting the provision of personal data to other countries. The main viewpoint in decision-making in this respect consists in the adequacy of legislative protection of personal data in the country to which the data are to be provided. Simultaneously, the decision-making process also encompasses the viewpoints specified in Article 12 of the Council of Europe Convention ETS No 108. In 2002, the Office dealt with a total of 149 applications for a permit to provide personal data abroad. It issued 138 decisions fully permitting the provision, 6 decisions rejecting the application in full and 3 final decisions that contained both favourable and rejecting standpoints.

In the field of international cooperation, the decision of the Article 29 Working Party of 13 December 2001 created an important new platform for the contact of representatives of independent bodies of supervision at the highest level of the Member States of the European Union and the candidate countries. The joint activities of representatives of independent authorities for data protection from the countries of central and eastern Europe, commenced in 2001 on the basis of an initiative of the Office and the Polish Office of the Inspector-General for Personal Data Protection, such as working meetings of the presidents and a joint website (www.ceecprivacy.org), intended to provide for mutual exchange of experience connected with preparation for accession to the European Union, were also continued. The Office organised the spring 2002 meeting in Prague. The one-year twinning project (CZ/2000/IB/OT/03) of expert assistance financed from the national Phare 2002 programme was completed in September 2002 and represented the climax of above-standard cooperation of the Office with the Spanish Agency for Protection of Data (APD).

In 2002, the efforts of the Office were concentrated on improving awareness of the Personal Data Protection Act amongst the general public and patient clarification of specific problems that were the subject of enquiries of citizens to the Office in relation to application of the act. The search for new potential for communication led, in particular, to the creation of a directory for direct contact with district, city and municipal authorities through e-mail. The Office considered the offer of direct contribution to application of legal regulations in the framework of its competence to be an effective service for the general public in places where the act is applied in everyday life. The extremely important communication with the media is

illustrated by the following table of 2002 contacts (press conferences, published daily press articles, interviews).

Agency service	14
Total press	87
Of which:	
daily press	76
periodicals	11
Television	66
Radio	23
Total media	**190**

Statistics on several other activities of the Office — 2002

Lectures, seminars	78
E-mail enquiries	1 500
Enquiries received by mail — legal persons	304
Enquiries received by mail — natural persons	117
Telephone enquiries	4 431
Total enquiries	**6 402**
Personal consultations provided to citizens and institutions	116
Contact with the media — agency service, press, radio and television	190
Regular press conferences of the Office	3
Materials published	
Journal of the Office (number of editions)	9
Bulletin of the Office (number of editions)	4
Standpoints/on practical issues	2/7
Press releases and communications for the press	16
Additional basic documents for the media	70
Total materials published	**108**
External hits of the website of the Office — daily average	105
Registration — total number of registrations	20 143
Control activities — Control Department and inspectors	354
Comments on legal regulations	
Acts	59
Decrees	48
Regulations of the government	19
Other	53
Total comments on legal regulations	**179**

As at 31 December 2002, the Office for Personal Data Protection had 71 employees.

The year 2003 was the last year of preparation for accession of the Czech Republic to the European Union. The Office for Personal Data Protection also consistently prepared for this new situation. An increased role within the Council of Europe, continued observer status in the Article 29 Working Party, or new representation in the common supervisory body for Europol and Schengen will undoubtedly impose high requirements on the employees of the Office after accession to the European Union. On the other hand, certain improvements in conditions under which the Office carried out its activities were achieved — the Office received new more suitable premises and its staff had grown at 31 December 2003 to 79 employees.

In 2003, the Office began to contribute to the improvement of personal data protection in the newly established European democracies. It participated in activities of the Council of Europe concerned with the Russian Federation, Bosnia and Herzegovina, and also Cyprus. For Bosnian protectors of personal data, it organised a workshop in Prague, while, in other cases, it contributed to the work of the expert group. This activity will undoubtedly be continued in the future. The Czech Republic is thus beginning to share its knowledge and experience in the area of personal data protection, which it obtained in the past from more experienced European countries.

In the area of foreign relations and international cooperation, the Office continues primarily to provide for fulfilment of requirements following from international treaties binding on the Czech Republic, as stipulated in Article 29(1)(g) of the Personal Data Protection Act. In connection with performance of the European (Association) Agreement, in the framework of its competence, the Office provides for harmonisation of the national legislation and the related practice with the law of the European Union, the *acquis communautaire*. In a fundamental document of the European Commission, consisting in the last year prior to accession of the Czech Republic to the European Union in the comprehensive monitoring report on the state of preparedness for EU membership of the Czech Republic, it is stated in Chapter 3, 'Free movement of services', that 'the Czech Republic has substantially harmonised its legislation in the area of personal data protection and free movement of these data. Nevertheless, certain modifications are required to harmonise the Personal Data Protection Act and the Act on Banks. The Office for Personal Data Protection has demonstrated that it is fully independent and efficient. Further employees will be required to ensure sustainable operation in the long term.' In relation to Chapter 24, 'Matters of justice and interior', there is a more favourable evaluation of the state of harmonisation of the legislation; however, the need for increasing the headcount by further recruiting is again mentioned.

In connection with the notes on the need for certain 'modifications' of the Personal Data Protection Act, the Office has drawn up a draft amendment to the act that should ensure final transposition of Directive 95/46/EC and simultaneously eliminate the incompatibility of Act No 21/1992 Coll. on Banks, as amended, from the viewpoint of personal data protection. The draft amendment to the two acts that was submitted to the Government of the Czech Republic on 30 September 2003 was based particularly on the results of working contacts with the relevant workplace in the framework of the Directorate-General for the Internal Market of the European Commission and also on certain results of cooperation with Spanish experts in the framework of the Phare twinning light project, which was completed in 2002. The Office cooperated with the Ministry of Informatics of the Czech Republic on transposition of the more recent legal regulation affecting the area of personal data protection — Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. In the framework of the European Union, the Office not only maintains contact and cooperates with the abovementioned Directorate-General for the Internal Market, but a representative of the Office also participated in four meetings of the Committee pursuant to Article 31 of Directive 95/46/EC, which is part of the European Commission and in which individual member countries are usually represented by a delegate of the governmental body responsible for implementing the governmental policy in the area of personal data protection. This has not yet been dealt with in the Czech Republic and in a number of other accession countries from the viewpoint of competence. The same is valid for cooperation in the framework of the Permanent Representatives Committee (Coreper), where the Office 'substitutes' for a governmental body, although it has not directly participated in its meetings to date. The Office directly cooperates particularly with the Ministry of the Interior and the Ministry of Finance of the Czech Republic. Cooperation was developed especially with the Ministry of the Interior in preparation of activities connected with the Schengen Agreement and Europol Agreement. These activities are concerned with future important and difficult agendas that will require specific solutions, both in the framework of domestic control activities and from

the viewpoint of international cooperation. In addition, the Office should be represented in the joint supervisory bodies (the Joint Supervisory Body and the Joint Supervisory Authority) in Brussels, which are active in connection both with the two abovementioned conventions within the competence of the Ministry of the Interior and with the Convention on the Use of Information Technology for Customs Purposes, which falls within the competence of the Ministry of Finance (the General Customs Directorate). Representatives of the Office have already participated as observers in a number of meetings of all three joint supervisory bodies.

In 2003, the Czech Republic was the fourth country which ratified the additional protocol to the Council of Europe Convention ETS No 108 regarding supervisory authorities and transborder data flows. At the same time, the ratification of the original convention was also extended to non-automated personal data processing.

The abovementioned extensive project of bilateral above-standard cooperation with the Spanish Agency for Protection of Data (APD), which was financed from the national Phare programme, and which was completed in September 2002, was an indirect basis for a new twinning light project commenced in 2003, agreed with the same foreign partner and again financed from the Phare funds. This six-month project which commenced in September 2003 should provide the Czech Office with the experience and knowledge required to fulfil its tasks in the area of electronic communication, Schengen cooperation, Europol and customs information systems.

Communication with the media continued even more extensively than in 2002 as illustrated by the following table of 2003 contacts (press conferences, published daily press articles, interviews).

Agency service	16
Total press	102
Of which:	
daily press	63
periodicals	39
Television	55
Radio	30
Basic documents for the media	89
Total media	292

Statistics on several other activities of the Office — 2003

Lectures, seminars	56
E-mail enquiries	892
Enquiries received by mail — legal persons	510
Enquiries received by mail — natural persons	424
Telephone enquiries	4 044
Total enquiries	**5 870**
Personal consultations provided to citizens and institutions	290
Contact with the media — agency service, press, radio and television	292
Regular press conferences of the Office	4
Materials published	
Journal of the Office (number of editions)	8
Bulletin of the Office (number of editions)	3
Standpoints/on practical issues	—/1
Translations of foreign documents	12
Press releases and communications for the press	10
Additional basic documents for the media	89
Total materials published	**123**

External hits of the website of the Office — daily average	95
Registration — total number of registrations	3 082
Comments on legislative drafts	
Acts	77
Decrees	74
Regulations of the government	26
Parliament documents	9
Other	41
Total comments on legislative drafts	**227**

As at 31 December 2003, the Office for Personal Data Protection had 79 employees.

Office for Personal Data Protection
Pplk. Sochora 27
CZ-17000 Prague 7
Tel. (420-2) 34 66 51 11
Fax (420-2) 34 66 54 44
E-mail: info@uoou.cz
Website: www.uoou.cz

Lithuania

The grounds for data protection are established in the Constitution of the Republic of Lithuania (1992) and in the law on legal protection of personal data of 1996. Although data protection is rather new in Lithuania and the increase in complaints is insignificant, still the interest of society in data protection is growing rapidly. The research for evaluation of the consequences of the implementation of Directive 95/46/EC and the Coucil of Europe Convention ETS No 108 carried out in the year 2002 presented unexpected results: more than a half of the citizens of Lithuania (61 %) were aware of personal data processing conditions and related rights.

Significant changes to privacy or data protection law in Lithuanian jurisdiction for the period 2002–03
At the beginning of the year 2002, the 'Strategic programme of the development of data protection in 2002–04' was ratified (Official Gazette, 2002, No 23-87).

The new version of the law on legal protection of personal data of the Republic of Lithuania was adopted in 2003 and from 1 July 2003 this law came into force. This law was passed in order to achieve fine-tuning with the EU *acquis*. The law establishes that the activities of the State Data Protection Inspectorate shall be based on the principles of lawfulness, impartiality, openness and professionalism in the discharge of its functions. When discharging the functions provided by this law and making its decisions related to the discharge of the functions set out for it in this law, the State Data Protection Inspectorate shall be independent; its rights may be limited only by law. State and municipal institutions and agencies, members of the *Seimas* and other officials, political parties, political and public organisations, and other legal and natural persons shall have no right to exert any kind of political, economic, psychological or social pressure on the employees of the State Data Protection Inspectorate or tamper with them in any other way. Interference with the activities of the State Data Protection Inspectorate shall render the infringing party liable in accordance with law. The English version of this law is available on the website at www.ada.lt.

Significant changes to other laws in Lithuania affecting privacy or data protection (either enhancement or otherwise)
The new version of the law on telecommunications, adopted on 26 July 2002, entered into force on 1 January 2003. This law contains special provisions concerning personal data processing and protection of privacy in the telecommunications sector.

The new version of the Penal Code, which entered into force on 1 May 2003, established penal liability for the unlawful collection of information about the private lives of individuals, disclosure and use of such information.

In June 2003, Parliament passed the resolution on the guaranteeing of personal data protection in the State institutions, taking into account that the State Data Protection Inspectorate established important and publicly discussed infringements of the law on legal protection of personal data in the information systems of the State institutions. This resolution brought the significance of data protection to the attention of the State institutions.

At the end of 2003, the *Seimas* of the Republic of Lithuania ratified the additional protocol to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) regarding supervisory authorities and transborder data flows.

Significant inquiries or reports in Lithuania that may affect privacy or data protection (for example, on new technologies, genetics, law enforcement/national security, community education, or self-help initiatives, etc.)
The main results of the Inspectorate's activity in 2002 are the following: it registered 1 004 personal data controllers during the year, investigated 21 complaints and applications, carried out 165 inspections, 1 324 consultations, prepared 5 methodical documents, prepared 3 and coordinated 20 legal acts, and coordinated 5 documents on information systems.

The results of the Inspectorate's activity in 2003 are the following: it examined 1 291 notifications on data processing of data controllers, examined 55 personal complaints (requests), executed 233 inspections and prepared 18 conclusions on prior checking, prepared 22 methodical documents, 95 legal acts and harmonised the documents provided by data controllers, gave 1 196 consultations, examined 7 requests on authorisation for transfer of data to foreign data recipients, and prepared 8 legal acts and 25 measures to inform the public.

Malta

The Data Protection Act which transposes Directive 95/46/EC was enacted in December 2001. Directive 2002/58/EC was transposed by regulations in 2003.

Both legislative instruments were brought into force on 15 July 2003.

Poland

Principal amendments to the legislation on personal data protection
The Inspector-General for the Protection of Personal Data has undertaken activities aimed at full adaptation of the provisions of the Polish Act on the Protection of Personal Data to the requirements 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. In 2003, the work on the amendment of the Act

on the Protection of Personal Data was continued, and the act was finally passed by Parliament in January 2004.

The draft amendment of the Act on the Protection of Personal Data provided, *inter alia*, for:

- introducing a provision ensuring free movement of personal data to the European Union and European Economic Area member countries, and therefore also defining the term 'third country', i.e. a country which is not a member of the EU or EEA;
- erasing the provisions which are inconsistent with Directive 95/46/EC, for example the provision which exempted the controller from the obligation to notify the data subject of his/her rights, the controller's address, etc.;
- introducing a provision concerning prior checking which apart from some exceptions covers the filing systems in which sensitive data are processed.

The amended Act on the Protection of Personal Data shall enter into force on the day the Republic of Poland acquires European Union membership.

Principal amendments to the legislation which influence privacy and personal data protection

On 1 January 2002, the Act on Access to Public Information (*Journal of Laws*, 2001, No 112, item 1198) entered into force. This act realises the principle of openness to the public of public life expressed in Article 61 of the Constitution of the Republic of Poland. The act specifies the basic rules of disclosure of public information, consultation of official documents and access to collective sessions of public authorities. The act determines a wide circle of subjects obliged to disclose such information. Limitation of the right of access to pubic information can be introduced exclusively by the provisions of statutory rank, *inter alia*, in view of the individual's privacy or the entrepreneur's secret.

On 18 July 2002, the Act on providing Services by Electronic Means was passed (*Journal of Laws*, 2002, No 144, item 1204). The act constitutes *lex specialis* in relation to the Act on the Protection of Personal Data. The provisions on personal data protection included in the Act on providing Services by Electronic Means apply exclusively to the data of consumers using this kind of service. The act regulates, *inter alia*, the scope of personal data which are necessary to enter into, shape the contents of, change or terminate a legal relationship between service provider and consumer, and electronic mail addresses of the consumer are expressly enumerated among these data. Pursuant to the Act on providing Services by Electronic Means, personal data are subject to protection irrespective of whether or not they are processed in the filing systems. Sending unsolicited commercial information, that is information to the receiving of which the recipient has not expressed his/her consent, shall be regarded as unfair competition practice.

On 14 February 2003, the Act on Disclosure of Economic Information was passed. This act specifies the rules and mode of disclosure of economic information concerning financial credibility of other entrepreneurs and consumers to third parties not indicated as recipients at the moment of deciding on disclosure of these data. The statutory definition of the term 'economic information' covers, *inter alia*, data concerning an individual, i.e. forename and surname, citizenship, address of permanent or temporary residence registration, personal identification number (PESEL number), series and number of identity card or other document proving one's identity, and date of birth. Economic information agencies process data according to the rules specified in the regulation which is subject to approval by the Minister for the Economy by way of administrative decision after consultation with the Inspector-General for the Protection of Personal Data.

New initiatives undertaken by the authority in order to provide help for organisations and authorities in fulfilling the obligations imposed by the provisions on personal data protection and to increase privacy protection

The Inspector-General for the Protection of Personal Data within the framework of its statutory obligations initiated and undertook activities aimed at improving personal data protection, *inter alia* by organising seminars, conferences and training, the main purpose of which was to enhance citizens' knowledge and legal awareness of personal data protection.

The Inspector-General has been conducting training in the field of personal data protection for government administration authorities, local government authorities and other interested parties (e.g. for persons in the banking and insurance sector). Moreover, the Inspector-General for the Protection of Personal Data, with the help of representatives of other data protection authorities, organised on 12 May 2003 in Gdynia the seminar 'Personal data protection and access to public information — Complementary or contradictory rights?', within the framework of the 'Academy for Personal Data Protection' — annual, one-day meetings available to everyone, devoted to the issues of personal data protection in different areas and in relation to various legal regulations. During the seminar, the problem of execution of the abovementioned right to public information and the provisions on personal data protection on the basis of the rich experience of the invited experts from the European Union member countries was discussed.

The Inspector-General also extended its website (www.giodo.gov.pl), which constitutes an interesting source of information in the field concerned (among other things a new site was added which concerns privacy protection in data communication systems and includes interesting guidelines and advice for users of these systems). The website is continually updated and is also available in English.

2.3. United States of America

On 13 February 2002, the European Commission published a staff working paper on the application of the Safe Harbour Decision (SEC(2002) 196). The staff working paper responded to Commissioner Bolkestein's undertaking, following the European Parliament's resolution of 5 July 2000 to make periodic reports to the Article 29 Working Party and to the relevant committee of the Parliament on the operation of the Safe Harbour Scheme.

The staff working paper concluded that on the EU side, Member States had put into place the necessary adjustments to their national laws to allow data to flow to organisations that self-certified their adherence to the Safe Harbour Scheme. On the US side, the paper reported that the Department of Commerce had set up a website containing extensive information on safe harbour rules, indications on how to join the scheme and the list of organisations that had self-certified. With regard to the level of protection provided for by the principles and its effective implementation by US organisations that had joined the Safe Harbour Scheme, the paper noted that not all the organisations had a visible privacy policy. Moreover, the paper noted that the safe harbour principles were not systematically reflected in organisations' posted privacy policies. Finally, the paper noted the lack of unresolved complaints.

3. ARTICLE 29 DATA PROTECTION WORKING PARTY

Members and observers for the years 2002 and 2003

Members

Austria	Belgium
Frau Dr Waltraut Kotschy Österreichische Datenschutzkommission Bundeskanzleramt Ballhausplatz 1 A-1014 Vienna Tel. (43-1) 531 15 26 79	Mr Paul Thomas President Commission de la protection de la vie privée Ministère de la Justice Boulevard de Waterloo 115 B-1000 Brussels Tel. (32-2) 542 72 00
Denmark	**Finland**
Mr Jacob Lundsager (1.2002–10.2002) Ms Janni Christoffersen (10.2002–) Director Datatilsynet Borgergade 28, Fifth floor DK-1300 Copenhagen V Tel. (45) 33 19 32 33	Mr Reijo Aarnio Data Protection Ombudsman Office of the Data Protection Ombudsman Ministry of Justice PO Box 315 FIN-00181 Helsinki Tel. (358-9) 182 51
France	**Germany**
Mr Marcel Pinet Conseiller d'État honoraire Commission nationale de l'informatique et des libertés (CNIL) 21, rue Saint Guillaume F-75340 Paris Cedex 7 Tel. (33) 153 73 22 31	Dr Joachim Jacob Der Bundesbeauftragte für den Datenschutz Friedrich-Ebert-Straße 1 D-53173 Bonn (Bad Godesberg) Tel. (49-228) 81 99 50
Greece	**Ireland**
Mr Constantin Dafermos (1.2002–9.2003) President Nikos Frangakis (11.2003–) Member Hellenic Data Protection Authority Ministry of Justice Kifisias Avenue 1–3 GR-11523 Athens (Ampelokipi) Tel. (30) 21 03 35 26 02	Mr Joe Meade Data Protection Commissioner Irish Life Centre, Block 6 Lower Abbey Street Dublin 1 Ireland Tel. (353-1) 874 85 44

Italy	Luxembourg
Prof. Stefano Rodotà President Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 I-00186 Rome Tel. (39) 06 69 67 77 03	Mr René Faber (1.2002–11.2002) President Commission à la protection des données nominatives Ministère de la Justice 15, boulevard Royal L-2934 Luxembourg Tel. (352) 48 71 80 Mr Gérard Lommel (11.2002–) President Commission nationale pour la protection des données 68, rue de Luxembourg L-4221 Esch-sur-Alzette Tel. (352) 26 10 60 20
Netherlands	**Portugal**
Mr Peter Hustinx President College bescherming persoonsgegevens (CBP) Prins Clauslaan 20 Postbus 93374 2509 AJ 's-Gravenhage Netherlands Tel. (31-70) 381 13 00	Mr Luís da Silveira President Comissão Nacional de Protecção de Dados Rua de S. Bento, 148 P-1200-821 Lisbon Codex Tel. (351) 213 92 84 00
Spain	**Sweden**
Mr José Luis Piñar Mañas Director Agencia de Protección de Datos C/ Sagasta, 22 E-28004 Madrid Tel. (34) 913 99 62 20	Mr Ulf Widebäck Director-General Datainspektionen Fleminggatan 14, Ninth floor Box 8114 S-104 20 Stockholm Tel. (46-8) 657 61 00
United Kingdom	
Mr Richard Thomas Information Commissioner Office of the Information Commissioner Executive Department Water Lane Wycliffe House Wilmslow Cheshire SK9 5AF United Kingdom Tel. (44-1625) 54 57 00 (switchboard)	

Observers

Iceland	Liechtenstein
Ms Sigrún Jóhannesdóttir Director Icelandic Data Protection Authority Raudararstigur 10 IS-105 Reykjavik Tel. (354) 560 90 10	Dr Philipp Mittelberger Data Protection Commissioner of the Principality of Liechtenstein Herrengasse 6 FL-9490 Vaduz Tel. (423) 236 60 90 Fax (423) 236 60 99 E-mail: info@sds.llv.li
Norway	**Cyprus**
Mr Georg Apenes Director-General Datatilsynet Data Inspectorate PB 8177 Dep. N-0034 Oslo Tel. (47) 22 39 69 00	Ms Goulla Frangou Commissioner for Personal Data Protection 40, Th. Dervis Street 1066 Nicosia Cyprus Tel. (357-22) 81 84 56 or 81 84 76 E-mail: commissioner@dataprotection.gov.cy
Czech Republic	**Estonia**
Dr Karel Neuwirt President Office for Personal Data Protection Pplk. Sochora 27 CZ-17000 Prague 7 Tel. (420-2) 34 66 51 11 Fax (420-2) 34 66 54 44 E-mail: karel.neuwirt@uoou.cz	Mr Urmas Kukk Director-General Estonian Data Protection Inspectorate Väike-Ameerika 19 EE-10129 Tallinn Tel. (372) 627 41 35 E-mail: urmas.kukk@dp.gov.ee
Hungary	**Latvia**
Mr Attila Peterfalvi Parliamentary Commissioner Office of the Parliamentary Commissioner for Data Protection and Freedom of Information Nádor u. 22. H-1051 Budapest Tel. (36-1) 475 71 86 E-mail: adatved@obh.hu	Ms Signe Plumina Director of the Data State Inspection Kr. Barona Street 5-4 LV-1050 Riga Tel. (371) 722 31 31 E-mail: signe@dvi.gov.lv
Lithuania	**Malta**
Ms Ona Jakstaite Director State Data Protection Inspectorate Gedimino Ave. 27/2 LT-2600 Vilnius Tel. (370-5) 212 75 32 E-mail: jakstaite@ada.lt	Mr Paul Mifsud-Cremona Commissioner for Data Protection Office of the Commissioner for Data Protection 280 Republic Street Valletta GPO 01 Malta Tel. (356) 21 22 16 24 E-mail: commissioner.dataprotection@gov.mt
Poland	**Romania**
Ms Ewa Kulesza Inspector-General Office of the Inspector-General for Personal Data Protection Stawki 2 PL-00193 Warsaw Tel. (48-22) 860 70 81 Fax (48-22) 860 70 90 E-mail: E_Kulesza@giodo.gov.pl	Mr Ioan Muraru Ombudsman Romanian People's Advocate Str. Eugen Carada, nr. 3, Sector 3 Bucharest Romania Tel. (40-21) 312 71 01 Fax (40-21) 312 49 21 E-mail: Avp@avp.ro

Slovakia	Slovenia
Mr Pavol Husar Office for the Protection of Personal Data Odborárske nám. 3 SK-81760 Bratislava Tel. (421-2) 50 23 94 18 Fax (421-2) 50 23 94 41 E-mail: pavol.husar@pdp.gov.sk	Mr Jernej Rovsek Deputy Ombudsman Republic of Slovenia Human Rights Ombudsman Dunajska 56 SLO-1109 Ljubljana Tel. (386-1) 475 00 20 E-mail: jernej.rovsek@varuh-rs.si

Documents adopted in 2002 and 2003 and website references

WP 54 (10557/02): Fifth annual report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the Community and in third countries covering the year 2000. Adopted on 6 March 2002.

WP 55 (5401/01): Recommendation on the surveillance of electronic communications in the workplace. Adopted on 29 May 2002.

WP 56 (5035/01): Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU-based websites. Adopted on 30 May 2002.

WP 57 (10761/02): Opinion 1/2002 on the CEN/ISSS report on privacy standardisation in Europe. Adopted on 30 May 2002.

WP 58 (10750/02): Opinion 2/2002 on the use of unique identifiers in telecommunication final equipment: the example of IPv6. Adopted on 30 May 2002.

WP 59 (11182/02): Internal report of the Internet Task Force on Microsoft.NET passport. Adopted on 2 July 2002.

WP 60 (11203/02): Working document — First orientations of the Article 29 Working Party concerning online authentication services. Adopted on 2 July 2002.

WP 61 (11190/02): Opinion 3/2002 on the data protection provisions of a Commission proposal for a directive on the harmonisation of the laws, regulations and administrative provisions of the Member States concerning credit for consumers. Adopted on 2 July 2002.

WP 62 (11194/02): Working document on functioning of the Safe Harbour Agreement. Adopted on 2 July 2002.

WP 63 (11081/02): Opinion 4/2002 on adequate level of protection of personal data in Argentina. Adopted on 3 October 2002.

WP 64: Opinion 5/2002 on the statement of the European data protection commissioners at the International Conference in Cardiff (9–11 September 2002) on Mandatory Systematic Retention of Telecommunication Traffic Data. Adopted on 11 October 2002.

WP 65 (11118/02): Working document on black lists. Adopted on 3 October 2002.

WP 66 (11647/02): Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States. Adopted on 24 October 2002.

WP 67 (11750/02): Working document on the processing of personal data by means of video surveillance. Adopted on 25 November 2002.

WP 68 (10054/03): Working document on online authentication services. Adopted on 29 January 2003.

WP 69 (12054/02): Opinion 1/2003 on the storage of traffic data for billing purposes. Adopted on 29 January 2003.

WP 70 (12251/03): Policy to promote the transparency of the activities of the Working Party established by Article 29 of Directive 95/46/EC. Adopted on 29 January 2003 (internal document).

WP 71: Work programme. Adopted on 25 February 2003.

WP 72 (10596/03): Note of the Secretariat on the state of play regarding the Safe Harbour Agreement (internal document).

WP 73 (10593/03): Working document on e-government. Adopted on 8 May 2003.

WP 74 (11639/02): Working document: Transfers of personal data to third countries: Applying Article 26(2) of the EU data protection directive to binding corporate rules for international data transfers.

WP 75 (11593/02): Working document on e-government. Adopted on 8 May 2003.

WP 76 (10972/03): Opinion 2/2003 on the application of the data protection principles to the Whois directories. Adopted on 13 June 2003.

WP 77 (10066/03): Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing. Adopted on 13 June 2003.

WP 78 (11070/03): Opinion 4/2003 on the level of protection ensured in the US for the transfer of passengers' data. Adopted on 13 June 2003.

WP 79 (10595/03): Opinion 5/2003 on the level of protection of personal data in Guernsey. Adopted on 13 June 2003.

WP 80 (12168/02): Working document on biometrics. Adopted on 1 August 2003.

WP 81: Internal report on workers' data protection in the employment context. Adopted on 24 September 2003 (internal document).

WP 82 (11580/03): Opinion 6/2003 on the level of protection of personal data in the Isle of Man. Adopted on 21 November 2003.

WP 83 (10936/03): Opinion 7/2003 on the reuse of public sector information and the protection of personal data. Adopted on 12 December 2003.

(12065/03): Sixth 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 2001. Adopted on 16 December 2003.

WP 84 (11754/03): Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business associations ('the alternative model contract'). Adopted on 17 December 2003.

The documents adopted by the Article 29 Working Party are available on the data protection website of the Directorate-General for the Internal Market on the Europa server of the European Commission at the following addresses:

http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2002/wpdocs02_en.htm
http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm

Data protection website: http://europa.eu.int/comm/privacy

41AS78_pages_limi_EN 21-01-2005 11:26 Pagina 3

European Commission

Seventh 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 years 2002 and 2003

Luxembourg: Office for Official Publications of the European Communities

2004 — 107 pp. — 17.6 x 25 cm

ISBN 92-894-6638-3